PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-087332
(43)Date of publication of application : 20.03.2003

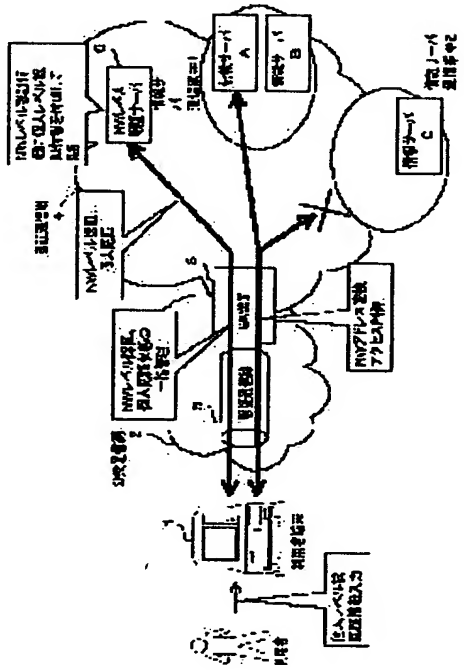
(51)Int.Cl. H04L 12/66

(21)Application number : 2001-277173
(22)Date of filing : 12.09.2001

(71)Applicant : NEC CORP
NTT COMMUNICATIONS KK
(72)Inventor : SUETSUGU TAKESHI
INOUE TAKUYA
YAMADA JUNNOSUKE
MIZOGUCHI YOICHI

(54) RELAY CONNECTION SYSTEM, NETWORK LEVEL AUTHENTICATION SERVER, GATEWAY, INFORMATION SERVER AND PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To allow an information server side to identify a user, to avoid dissidence or duplication of an authentication state in an authentication communication network, to simplify the procedure of the authentication at a network level or a personal level and to relieve the processing load imposed on a gateway.
SOLUTION: The network level authentication server stores authentication information resulting from attaching personal level authentication information to network level authentication information and personal level access control information, checks information to be authenticated received from a user terminal, attaches the access control information to the authentication result and transfers the result to the gateway. The gateway stores both a network address and a user identifier at the completion of authentication and stores the personal level access control information corresponding to them. The gateway retrieves corresponding access control information from a network address of the user terminal at the access from the user terminal to the authentication communication network and controls the access of the user terminal to the information server according to the access control information.



LEGAL STATUS

[Date of request for examination] 19.09.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3645844

[Date of registration] 10.02.2005

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－87332
（P2003－87332A）
(43)公開日　平成15年３月20日(2003.3.20)

(51)Int.Cl.'	識別記号	ＦＩ	テーマコード'（参考）
Ｈ０４Ｌ　12/66		Ｈ０４Ｌ　12/66	Ｂ　５Ｋ０３０

審査請求　有　　請求項の数30　ＯＬ　（全 31 頁）

(21)出願番号　特願2001－277173(P2001－277173)

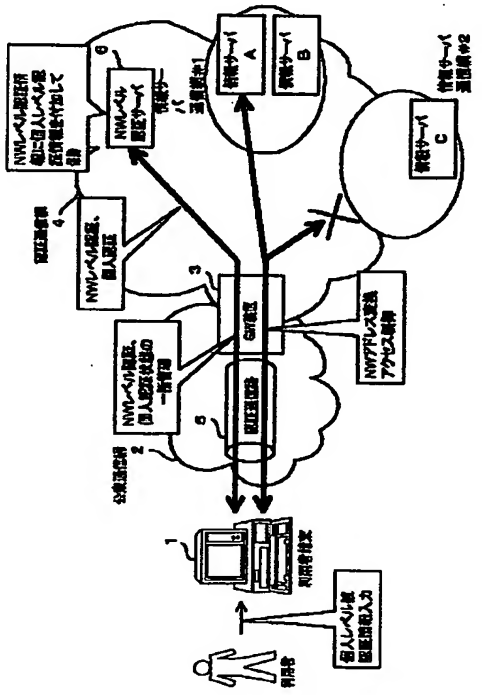
(22)出願日　平成13年９月12日(2001.9.12)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(71)出願人　399035766
エヌ・ティ・ティ・コミュニケーションズ株式会社
東京都千代田区内幸町一丁目１番６号
(72)発明者　末次　剛
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100078237
弁理士　井出　直孝　（外１名）

最終頁に続く

(54)【発明の名称】　中継接続方式およびネットワークレベル認証サーバおよびゲートウェイ装置および情報サーバおよびプログラム

(57)【要約】
【課題】　情報サーバ側から利用者を特定する。認証通信網内における認証状態の不一致または重複を回避する。ネットワークレベル認証および個人レベル認証の手順を簡単化する。ゲートウェイ装置の処理負荷を軽減させる。
【解決手段】　ネットワークレベル認証サーバは、ネットワークレベルの認証情報に個人レベルの認証情報を付加した認証情報および個人レベルのアクセス制御情報を保持し、利用者端末から受信した被認証情報を検証しその認証結果にアクセス制御情報を付加してゲートウェイ装置に転送する。ゲートウェイ装置は、認証の完了時にネットワークアドレスおよび利用者識別子をそれぞれを保持するとともにこれらに対応して個人レベルのアクセス制御情報を保持する。利用者端末からの認証通信網へのアクセス時に利用者端末のネットワークアドレスから該当するアクセス制御情報を検索しこのアクセス制御情報にしたがって利用者端末の情報サーバに対するアクセスを制御する。



1

【特許請求の範囲】

【請求項１】　ネットワークレベルおよび個人レベルでの認証の双方を行った利用者が利用可能でありプライベートネットワークアドレスにより制御され利用者に情報を提供する情報サーバを含む私設通信網としての認証通信網と、

この認証通信網にアクセスする利用者端末に接続された公衆通信網と前記認証通信網とを接続するゲートウェイ装置とを備えた中継接続方式において、

ネットワークレベルの認証情報に個人レベルの認証情報を付加した認証情報を保持するネットワークレベル認証サーバが設けられ、

前記ネットワークレベル認証サーバは、

前記認証情報と併せて個人レベルのアクセス制御情報も付加して保持する手段と、

前記ゲートウェイ装置から認証要求として受信した被認証情報を検証しその認証結果に前記アクセス制御情報を付加して前記ゲートウェイ装置に返送する手段とを備え、

前記ゲートウェイ装置は、

ネットワークレベルの被認証情報に個人レベルの被認証情報を付加した被認証情報および利用者識別子とこの被認証情報の有効期限情報とを前記利用者端末から受信して前記有効期限を検証して前記被認証情報の有効性を確認する手段と、前記利用者識別子および前記被認証情報を用いて前記ネットワークレベル認証サーバに対して前記認証要求を送信する手段と、

認証の完了時に認証通信網内部で使用するプライベートネットワークアドレスを前記利用者端末の利用者に割当てこのプライベートネットワークアドレスと前記ネットワークレベル認証サーバから前記認証結果として返送されたネットワークレベルの認証情報および個人レベルの認証情報としての前記利用者の公衆通信網におけるアドレスであるネットワークアドレスおよび利用者識別子をそれぞれ保持するとともにこれらに対応して前記ネットワークレベル認証サーバから前記認証結果とともに返送された前記個人レベルのアクセス制御情報を保持する手段と、

認証の完了時に、前記利用者との間に相互に秘密情報を共有してこの秘密情報を利用した暗号通信路である認証通信路を前記利用者端末との間に生成する手段と、

前記利用者からの認証通信網内へのアクセスについては前記認証通信路に限定して許容するとともに前記公衆通信網におけるネットワークアドレスと前記認証通信網内部で利用するプライベートアドレスとの間でアドレス変換を行う手段と、

前記利用者からの前記認証通信網へのアクセス時に前記利用者のネットワークアドレスから該当する前記アクセス制御情報を検索しこのアクセス制御情報にしたがって前記利用者の前記情報サーバに対するアクセスを制御する手段とを備えたことを特徴とする中継接続方式。

2

【請求項２】　前記情報サーバは、前記利用者からアクセスがあるときには前記利用者のプライベートネットワークアドレスを用いて前記ゲートウェイ装置に当該利用者の個人認証状態を問い合わせることにより前記利用者識別子を取得する手段を備えた請求項１記載の中継接続方式。

【請求項３】　前記ゲートウェイ装置は、前記情報サーバが個人レベルの認証状態を解放するまで当該利用者に割当てた前記認証通信網内のプライベートネットワークアドレスの再割り当てを行わない手段を備えた請求項１記載の中継接続方式。

【請求項４】　前記ゲートウェイ装置は、利用者からの要求に応じて、もしくは、利用者から前記認証通信路を利用した前記認証通信網内部への一定時間以上の無通信を検出した時点で前記認証通信路を削除する手段を備えた請求項１記載の中継接続方式。

【請求項５】　前記ゲートウェイ装置は、前記認証通信路の削除を行う際に、当該認証通信路の利用者の利用していた前記情報サーバに対して当該認証通信路の削除と個人レベルの認証状態の解放とを通知する手段を備え、

前記情報サーバは、前記ゲートウェイ装置からの前記通知により該当する利用者の個人レベルの認証状態を解放する手段を備えた請求項１記載の中継接続方式。

【請求項６】　前記ゲートウェイ装置は、利用者からの前記認証通信路の設定要求を受信した際に、前記ネットワークレベル認証サーバに対してこの設定要求に含まれる利用者識別子および被認証情報および前記利用者のネットワークアドレスを前記認証要求に設定して前記ネットワークレベル認証サーバに送信する手段を備え、

前記ネットワークレベル認証サーバは、

前記認証要求を受信して前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子を保持する手段と、

前記認証要求を受信して当該ネットワークレベル認証サーバにより保持されている通信中の前記認証通信路の情報を検索して前記認証要求中に設定されている前記利用者識別子およびまたは前記ネットワークアドレスにしたがって既に前記認証通信路が設定されているか否かを検出する手段と、

同一の前記利用者識別子もしくは前記ネットワークアドレスにより既に前記認証通信路が設定されているときには当該認証通信路を設定している前記ゲートウェイ装置に対して重複する前記認証通信路の削除要求を送信する手段とを備え、

前記ゲートウェイ装置は、

前記認証通信路の削除要求を受信して該当する認証通信路を検索する手段と、この検索する手段の検索結果により前記該当する認証通信路が検索されたときにはその認証通信路を削除して当該削除完了の応答を前記ネットワ

ークレベル認証サーバに通知する手段とを備え、
前記ネットワークレベル認証サーバは、同一の前記利用者識別子もしくは前記ネットワークアドレスにより既に前記認証通信路が設定されていないとき、もしくは、前記削除完了の応答を受信したときには前記認証要求に設定されている前記利用者識別子および前記被認証情報を検証してこの認証の結果に該当利用者のアドレス制御情報を付加して応答する手段を備え、
前記ゲートウェイ装置は、
このアドレス制御情報が付加された応答を受信して前記認証通信路を設定する手段と、
当該認証通信路設定の通知を前記ネットワークレベル認証サーバに送信する手段とを備え、
前記ネットワークレベル認証サーバは、前記認証通信路設定の通知を受信して設定済みの認証通信路情報として前記認証通信路を設定した前記ゲートウェイ装置の識別情報および前記利用者識別子および前記ネットワークアドレスをそれぞれ自己内部に保持する手段を備え、
前記ゲートウェイ装置は、
前記利用者からの要求に応じて、もしくは、前記利用者から前記認証通信路を利用した前記認証通信網内部への一定時間以上の無通信を検出したときに前記認証通信路を削除する手段と、
自己内部に保持している該当認証通信路に関する情報を破棄する手段と、
該当認証通信路の削除を前記ネットワークレベル認証サーバに通知する手段とを備え、
前記ネットワークレベル認証サーバは、この削除の通知を受信して該当する認証通信路に関する情報を破棄する手段を備えたことを特徴とする請求項１記載の中継接続方式。

【請求項７】　前記ゲートウェイ装置は、認証完了後に前記認証通信路を確立した利用者のネットワークアドレスおよびこのネットワークアドレスに対応する利用者識別子を保持する手段と、
前記認証通信路の設定要求を受信したときに現在自己が設定している前記認証通信路を利用している利用者のネットワークアドレスおよびまたはこのネットワークアドレスに対応する利用者識別子を検索する手段と、
この検索する手段の検索結果により前記設定要求に含まれる利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子と現在自己が設定している前記認証通信路を利用している利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子とが同一であるときには前記自己が設定している既存の前記認証通信路を削除して前記設定要求に基づく前記認証通信路を設定する手段と、
前記検索する手段の検索結果により前記設定要求に含まれる利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子と現在自己が設定している前記認証通信路を利用している利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子とが一致しないときには他の前記ゲートウェイ装置に前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子を通知する手段と、
この通知を他のゲートウェイ装置から受信したときには自己が保持している前記認証通信路設定中の利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子が前記通知に含まれる前記ネットワークアドレスおよびまたは前記利用者識別子と同一であるか否かを検索する手段と、
この検索する手段の検索結果が同一でないときにはその旨を前記通知の送信元の前記ゲートウェイ装置に応答する手段と、
前記検索する手段の検索結果が同一であるときには自己が保持する重複する前記認証通信路を削除するとともに自己が保持している重複する前記認証通信路に関する情報を破棄する手段と、
前記通知の送信元に重複する前記認証通信路の該当利用者有りおよび削除完了の旨を応答する手段と、
自己が前記通知の送信元であり前記応答を受信したときには新規の前記認証通信路を設定する手段とを備えた請求項１記載の中継接続方式。

【請求項８】　前記ゲートウェイ装置は、認証完了後に前記認証通信路を確立した利用者のネットワークアドレスおよびこのネットワークアドレスに対応する利用者識別子を保持する手段と、
前記認証通信路の設定要求を受信したときに現在自己が設定している前記認証通信路を利用している利用者のネットワークアドレスおよびまたはこのネットワークアドレスに対応する利用者識別子を検索する手段と、
この検索する手段の検索結果により前記設定要求に含まれる利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子と現在自己が設定している前記認証通信路を利用している利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子とが同一であるときには前記自己が設定している既存の前記認証通信路を削除して前記設定要求に基づく前記認証通信路を設定する手段と、
前記検索する手段の検索結果により前記設定要求に含まれる利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子と現在自己が設定している前記認証通信路を利用している利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子とが一致しないときには他の前記ゲートウェイ装置に前記ネットワークアドレスおよびこのネットワークアドレスに対

応する前記利用者識別子を通知する手段と、
この通知を他のゲートウェイ装置から受信したときには自己が保持している前記認証通信路設定中の利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子が前記通知に含まれる前記ネットワークアドレスおよびまたは前記利用者識別子と同一であるか否かを検索する手段と、
この検索する手段の検索結果が同一でないときにはその旨を前記通知の送信元の前記ゲートウェイ装置に応答する手段と、
前記検索する手段の検索結果が同一であるときにはその旨を前記通知の送信元の前記ゲートウェイ装置に応答する手段と、
自己が前記通知の送信元でありこの応答を受信したときにはこの応答の送信元の前記ゲートウェイ装置に対して当該ゲートウェイ装置が保持する重複する前記認証通信路を削除するとともに当該ゲートウェイ装置が保持している重複する前記認証通信路に関する情報を削除する要求を行う手段と、
自己が前記応答の送信元でありこの要求を受信したときには自己が保持する重複する前記認証通信路を削除するとともに自己が保持している重複する前記認証通信路に関する情報を破棄する手段と、
前記要求の送信元に重複する前記認証通信路の該当利用者有りおよび削除完了の旨を応答する手段と、
自己が前記要求の送信元であり前記応答を受信したときには新規の前記認証通信路を設定する手段とを備えた請求項１記載の中継接続方式。
【請求項９】　前記ゲートウェイ装置は、
認証完了後に前記認証通信路を確立した利用者のネットワークアドレスおよびこのネットワークアドレスに対応する利用者識別子を保持する手段と、
この保持する手段に保持した前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子の情報を他の前記ゲートウェイ装置に通知する手段と、
この通知を他の前記ゲートウェイ装置から受けたときには当該認証通信路を設定している前記ゲートウェイ装置の情報および前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子の情報を保持する手段と、
前記認証通信路の設定要求を受信したときには現在自己が保持している全ての前記ゲートウェイ装置で設定されている前記認証通信路を利用している利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子を検索しいずれかが同一のときにはその認証通信路を設定している前記ゲートウェイ装置を確認する手段と、
当該認証通信路を設定している前記ゲートウェイ装置が自己であるときには該当する前記認証通信路を削除する

とともに新規に要求された前記認証通信路を設定する手段と、
当該認証通信路を設定している前記ゲートウェイ装置が他の前記ゲートウェイ装置であるときには該当する前記ゲートウェイ装置に対して前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子を設定して前記認証通信路の削除要求を送信する手段と、
自己がこの削除要求を受信したときには、要求中の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子と一致する前記認証通信路を検索してこれを削除し削除完了の旨を前記削除要求元の前記ゲートウェイ装置に応答する手段と、
自己が前記削除要求元でありこの削除完了応答を受信したときには、新規に要求のあった前記認証通信路を設定する手段とを備えた請求項１記載の中継接続方式。
【請求項１０】　個人認証の実施がアプリケーションレベルに限定された情報サーバが設けられ、
前記ゲートウェイ装置と当該情報サーバとの間にアクセス制御サーバが設けられ、
このアクセス制御サーバは、
利用者のプライベートアドレスを用いて前記ゲートウェイ装置にこの利用者の個人認証状態を問い合わせることによりこの利用者の利用者識別子を取得する手段と、
前記情報サーバに前記アプリケーションレベルでの個人認証情報としての利用者識別子を送信する手段と
を備えた請求項１記載の中継接続方式。
【請求項１１】　前記アクセス制御サーバは、
前記個人認証情報を元に前記利用者に対応するアプリケーションを認識する手段と、
この認識する手段により認識したアプリケーションにしたがって前記情報サーバに対してこのアプリケーションレベルでのアクセス制御を行う手段とを備えた請求項１０記載の中継接続方式。
【請求項１２】　請求項１ないし１１のいずれかに記載の中継接続方式に適用され、
ネットワークレベルの認証情報に個人レベルの認証情報を付加した認証情報を保持する手段と、
前記認証情報と併せて個人レベルのアクセス制御情報も付加して保持する手段と、
前記ゲートウェイ装置から認証要求として受信した被認証情報を検証しその認証結果に前記アクセス制御情報を付加して前記ゲートウェイ装置に返送する手段とを備えたことを特徴とするネットワークレベル認証サーバ。
【請求項１３】　前記ゲートウェイ装置が利用者からの前記認証通信路の設定要求を受信した際にこの設定要求に含まれる利用者識別子および被認証情報および前記利用者のネットワークアドレスを設定した前記認証要求を受信して前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子を保持する手

段と、
前記認証要求を受信して保持されている通信中の前記認証通信路の情報を検索して前記認証要求中に設定されている前記利用者識別子およびまたは前記ネットワークアドレスにしたがって既に前記認証通信路が設定されているか否かを検出する手段と、
同一の前記利用者識別子もしくは前記ネットワークアドレスにより既に前記認証通信路が設定されているときには当該認証通信路を設定している前記ゲートウェイ装置に対して重複する前記認証通信路の削除要求を送信する手段と、
同一の前記利用者識別子もしくは前記ネットワークアドレスにより既に前記認証通信路が設定されていないとき、もしくは、前記削除完了の応答を受信したときには前記認証要求に設定されている前記利用者識別子および前記被認証情報を検証してこの認証の結果に該当利用者のアドレス制御情報を付加して前記認証要求または前記削除完了の応答を送信したゲートウェイ装置に応答する手段と、
前記ゲートウェイ装置からの前記認証通信路設定の通知を受信して設定済みの認証通信路情報として前記認証通信路を設定した前記ゲートウェイ装置の識別情報および前記利用者識別子および前記ネットワークアドレスをそれぞれ自己内部に保持する手段と、
前記ゲートウェイ装置からの前記認証通信路の削除の通知を受信して該当する認証通信路に関する情報を破棄する手段とを備えた請求項１２記載のネットワークレベル認証サーバ。
【請求項１４】　請求項１ないし１１のいずれかに記載の中継接続方式に適用され、
ネットワークレベルの被認証情報に個人レベルの被認証情報を付加した被認証情報および利用者識別子とこの被認証情報の有効期限情報とを前記利用者端末から受信して前記有効期限を検証して前記被認証情報の有効性を確認する手段と、
前記利用者識別子および前記被認証情報を用いて前記ネットワークレベル認証サーバに対して前記認証要求を送信する手段と、
認証の完了時に認証通信網内部で使用するプライベートネットワークアドレスを前記利用者に割当てこのプライベートネットワークアドレスと前記ネットワークレベル認証サーバから前記認証結果として返送されたネットワークレベルの認証情報および個人レベルの認証情報としての前記利用者の公衆通信網におけるアドレスであるネットワークアドレスおよび利用者識別子をそれぞれ保持するとともにこれらに対応して前記ネットワークレベル認証サーバから前記認証結果とともに返送された前記個人レベルのアクセス制御情報を保持する手段と、
認証の完了時に、前記利用者との間に相互に秘密情報を共有してこの秘密情報を利用した暗号通信路である認証通信路を前記利用者端末との間に生成する手段と、
前記利用者からの認証通信網内へのアクセスについては前記認証通信路に限定して許容するとともに前記公衆通信網におけるネットワークアドレスと前記認証通信網内部で利用するプライベートアドレスとの間でアドレス変換を行う手段と、
前記利用者からの前記認証通信網へのアクセス時に前記利用者のネットワークアドレスから該当する前記アクセス制御情報を検索しこのアクセス制御情報にしたがって前記利用者の前記情報サーバに対するアクセスを制御する手段とを備えたことを特徴とするゲートウェイ装置。
【請求項１５】　認証完了後に前記認証通信路を確立した利用者のネットワークアドレスおよびこのネットワークアドレスに対応する利用者識別子を保持する手段と、
前記認証通信路の設定要求を受信したときに現在自己が設定している前記認証通信路を利用している利用者のネットワークアドレスおよびまたはこのネットワークアドレスに対応する利用者識別子を検索する手段と、
この検索する手段の検索結果により前記設定要求に含まれる利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子と現在自己が設定している前記認証通信路を利用している利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子とが同一であるときには前記自己が設定している既存の前記認証通信路を削除して前記設定要求に基づく前記認証通信路を設定する手段と、
前記検索する手段の検索結果により前記設定要求に含まれる利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子と現在自己が設定している前記認証通信路を利用している利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子とが一致しないときには他の前記ゲートウェイ装置に前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子を通知する手段と、
この通知を他のゲートウェイ装置から受信したときには自己が保持している前記認証通信路設定中の利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子が前記通知に含まれる前記ネットワークアドレスおよびまたは前記利用者識別子と同一であるか否かを検索する手段と、
この検索する手段の検索結果が同一でないときにはその旨を前記通知の送信元の前記ゲートウェイ装置に応答する手段と、
前記検索する手段の検索結果が同一であるときには自己が保持する重複する前記認証通信路を削除するとともに自己が保持している重複する前記認証通信路に関する情報を破棄する手段と、
前記通知の送信元に重複する前記認証通信路の該当利用

者有りおよび削除完了の旨を応答する手段と、
自己が前記通知の送信元であり前記応答を受信したときには新規の前記認証通信路を設定する手段とを備えた請求項１４記載のゲートウェイ装置。
【請求項１６】　認証完了後に前記認証通信路を確立した利用者のネットワークアドレスおよびこのネットワークアドレスに対応する利用者識別子を保持する手段と、
前記認証通信路の設定要求を受信したときに現在自己が設定している前記認証通信路を利用している利用者のネットワークアドレスおよびまたはこのネットワークアドレスに対応する利用者識別子を検索する手段と、
この検索する手段の検索結果により前記設定要求に含まれる利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子と現在自己が設定している前記認証通信路を利用している利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子とが同一であるときには前記自己が設定している既存の前記認証通信路を削除して前記設定要求に基づく前記認証通信路を設定する手段と、
前記検索する手段の検索結果により前記設定要求に含まれる利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子と現在自己が設定している前記認証通信路を利用している利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子とが一致しないときには他の前記ゲートウェイ装置に前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子を通知する手段と、
この通知を他のゲートウェイ装置から受信したときには自己が保持している前記認証通信路設定中の利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子が前記通知に含まれる前記ネットワークアドレスおよびまたは前記利用者識別子と同一であるか否かを検索する手段と、
この検索する手段の検索結果が同一でないときにはその旨を前記通知の送信元の前記ゲートウェイ装置に応答する手段と、
前記検索する手段の検索結果が同一であるときにはその旨を前記通知の送信元の前記ゲートウェイ装置に応答する手段と、
自己が前記通知の送信元でありこの応答を受信したときにはこの応答の送信元の前記ゲートウェイ装置に対して当該ゲートウェイ装置が保持する重複する前記認証通信路を削除するとともに当該ゲートウェイ装置が保持している重複する前記認証通信路に関する情報を削除する要求を行う手段と、
自己が前記応答の送信元でありこの要求を受信したときには自己が保持する重複する前記認証通信路を削除するとともに自己が保持している重複する前記認証通信路に関する情報を破棄する手段と、
前記要求の送信元に重複する前記認証通信路の該当利用者有りおよび削除完了の旨を応答する手段と、
自己が前記要求の送信元であり前記応答を受信したときには新規の前記認証通信路を設定する手段とを備えた請求項１４記載のゲートウェイ装置。
【請求項１７】　認証完了後に前記認証通信路を確立した利用者のネットワークアドレスおよびこのネットワークアドレスに対応する利用者識別子を保持する手段と、
この保持する手段に保持した前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子の情報を他の前記ゲートウェイ装置に通知する手段と、
この通知を他の前記ゲートウェイ装置から受けたときには当該認証通信路を設定している前記ゲートウェイ装置の情報および前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子の情報を保持する手段と、
前記認証通信路の設定要求を受信したときには現在自己が保持している全ての前記ゲートウェイ装置で設定されている前記認証通信路を利用している利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子を検索しいずれかが同一のときにはその認証通信路を設定している前記ゲートウェイ装置を確認する手段と、
当該認証通信路を設定している前記ゲートウェイ装置が自己であるときには該当する前記認証通信路を削除するとともに新規に要求された前記認証通信路を設定する手段と、
当該認証通信路を設定している前記ゲートウェイ装置が他の前記ゲートウェイ装置であるときには該当する前記ゲートウェイ装置に対して前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子を設定して前記認証通信路の削除要求を送信する手段と、
自己がこの削除要求を受信したときには、要求中の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子と一致する前記認証通信路を検索してこれを削除し削除完了の旨を前記削除要求元の前記ゲートウェイ装置に応答する手段と、
自己が前記削除要求元でありこの削除完了応答を受信したときには、新規に要求のあった前記認証通信路を設定する手段とを備えた請求項１４記載のゲートウェイ装置。
【請求項１８】　請求項１ないし１１のいずれかに記載の中継接続方式に適用され、
前記利用者からアクセスがあるときには前記利用者のプライベートネットワークアドレスを用いて前記ゲートウェイ装置に当該利用者の個人認証状態を問い合わせることにより前記利用者識別子を取得する手段を備えたこと

を特徴とする情報サーバ。

【請求項１９】　請求項１ないし１１のいずれかに記載の中継接続方式に適用され、

前記ゲートウェイ装置と個人認証の実施がアプリケーションレベルに限定された情報サーバとの間に設けられ、

利用者のプライベートアドレスを用いて前記ゲートウェイ装置にこの利用者の個人認証状態を問い合わせることによりこの利用者の利用者識別子を取得する手段と、

前記情報サーバに前記アプリケーションレベルでの個人認証情報としての利用者識別子を送信する手段とを備えたことを特徴とするアクセス制御サーバ。

【請求項２０】　前記個人認証情報を元に前記利用者に対応するアプリケーションを認識する手段と、

この認識する手段により認識したアプリケーションにしたがって前記情報サーバに対してこのアプリケーションレベルでのアクセス制御を行う手段とを備えた請求項１９記載のアクセス制御サーバ。

【請求項２１】　情報処理装置にインストールすることにより、その情報処理装置に、請求項１ないし１１のいずれかに記載の中継接続方式に適用される前記ネットワークレベル認証サーバに相応する機能として、

ネットワークレベルの認証情報に個人レベルの認証情報を付加した認証情報を保持する機能と、

前記認証情報と併せて個人レベルのアクセス制御情報も付加して保持する機能と、

前記ゲートウェイ装置から認証要求として受信した被認証情報を検証しその認証結果に前記アクセス制御情報を付加して前記ゲートウェイ装置に返送する機能とを実現させることを特徴とするプログラム。

【請求項２２】　前記ゲートウェイ装置が利用者からの前記認証通信路の設定要求を受信した際にこの設定要求に含まれる利用者識別子および被認証情報および前記利用者のネットワークアドレスを設定した前記認証要求を受信して前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子を保持する機能と、

前記認証要求を受信して保持されている通信中の前記認証通信路の情報を検索して前記認証要求中に設定されている前記利用者識別子およびまたは前記ネットワークアドレスにしたがって既に前記認証通信路が設定されているか否かを検出する機能と、

同一の前記利用者識別子もしくは前記ネットワークアドレスにより既に前記認証通信路が設定されているときには当該認証通信路を設定している前記ゲートウェイ装置に対して重複する前記認証通信路の削除要求を送信する機能と、

同一の前記利用者識別子もしくは前記ネットワークアドレスにより既に前記認証通信路が設定されていないとき、もしくは、前記削除完了の応答を受信したときには前記認証要求に設定されている前記利用者識別子および前記被認証情報を検証してこの認証の結果に該当利用者のアドレス制御情報を付加して前記認証要求または前記削除完了の応答を送信したゲートウェイ装置に応答する機能と、

前記ゲートウェイ装置からの前記認証通信路設定の通知を受信して設定済みの認証通信路情報として前記認証通信路を設定した前記ゲートウェイ装置の識別情報および前記利用者識別子および前記ネットワークアドレスをそれぞれ自己内部に保持する機能と、

前記ゲートウェイ装置からの前記認証通信路の削除の通知を受信して該当する認証通信路に関する情報を破棄する機能とを実現させる請求項２１記載のプログラム。

【請求項２３】　情報処理装置にインストールすることにより、その情報処理装置に、請求項１ないし１１のいずれかに記載の中継接続方式に適用される前記ゲートウェイ装置に相応する機能として、

ネットワークレベルの被認証情報に個人レベルの被認証情報を付加した被認証情報および利用者識別子とこの被認証情報の有効期限情報とを前記利用者端末から受信して前記有効期限を検証して前記被認証情報の有効性を確認する機能と、

前記利用者識別子および前記被認証情報を用いて前記ネットワークレベル認証サーバに対して前記認証要求を送信する機能と、

認証の完了時に認証通信網内部で使用するプライベートネットワークアドレスを前記利用者に割当てこのプライベートネットワークアドレスと前記ネットワークレベル認証サーバから前記認証結果として返送されたネットワークレベルの認証情報および個人レベルの認証情報としての前記利用者の公衆通信網におけるアドレスであるネットワークアドレスおよび利用者識別子をそれぞれ保持するとともにこれらに対応して前記ネットワークレベル認証サーバから前記認証結果とともに返送された前記個人レベルのアクセス制御情報を保持する機能と、

認証の完了時に、前記利用者との間に相互に秘密情報を共有し、この秘密情報を利用した暗号通信路である認証通信路を前記利用者端末との間に生成する機能と、

前記利用者からの認証通信網内へのアクセスについては前記認証通信路に限定して許容するとともに前記公衆通信網におけるネットワークアドレスと前記認証通信網内部で利用するプライベートアドレスとの間でアドレス変換を行う機能と、

前記利用者からの前記認証通信網へのアクセス時に前記利用者のネットワークアドレスから該当する前記アクセス制御情報を検索しこのアクセス制御情報にしたがって前記利用者の前記情報サーバに対するアクセスを制御する機能とを実現させることを特徴とするプログラム。

【請求項２４】　認証完了後に前記認証通信路を確立した利用者のネットワークアドレスおよびこのネットワークアドレスに対応する利用者識別子を保持する機能と、

前記認証通信路の設定要求を受信したときに現在自己が設定している前記認証通信路を利用している利用者のネットワークアドレスおよびまたはこのネットワークアドレスに対応する利用者識別子を検索する機能と、
この検索する機能の検索結果により前記設定要求に含まれる利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子と現在自己が設定している前記認証通信路を利用している利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子とが同一であるときには前記自己が設定している既存の前記認証通信路を削除して前記設定要求に基づく前記認証通信路を設定する機能と、
前記検索する機能の検索結果により前記設定要求に含まれる利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子と現在自己が設定している前記認証通信路を利用している利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子とが一致しないときには他の前記ゲートウェイ装置に前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子を通知する機能と、
この通知を他のゲートウェイ装置から受信したときには自己が保持している前記認証通信路設定中の利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子が前記通知に含まれる前記ネットワークアドレスおよびまたは前記利用者識別子と同一であるか否かを検索する機能と、
この検索する機能の検索結果が同一でないときにはその旨を前記通知の送信元の前記ゲートウェイ装置に応答する機能と、
前記検索する機能の検索結果が同一であるときには自己が保持する重複する前記認証通信路を削除するとともに自己が保持している重複する前記認証通信路に関する情報を破棄する機能と、
前記通知の送信元に重複する前記認証通信路の該当利用者有りおよび削除完了の旨を応答する機能と、
自己が前記通知の送信元であり前記応答を受信したときには新規の前記認証通信路を設定する機能とを実現させる請求項２３記載のプログラム。

【請求項２５】　認証完了後に前記認証通信路を確立した利用者のネットワークアドレスおよびこのネットワークアドレスに対応する利用者識別子を保持する機能と、
前記認証通信路の設定要求を受信したときに現在自己が設定している前記認証通信路を利用している利用者のネットワークアドレスおよびまたはこのネットワークアドレスに対応する利用者識別子を検索する機能と、
この検索する機能の検索結果により前記設定要求に含まれる利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子と

現在自己が設定している前記認証通信路を利用している利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子とが同一であるときには前記自己が設定している既存の前記認証通信路を削除して前記設定要求に基づく前記認証通信路を設定する機能と、
前記検索する機能の検索結果により前記設定要求に含まれる利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子と現在自己が設定している前記認証通信路を利用している利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子とが一致しないときには他の前記ゲートウェイ装置に前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子を通知する機能と、
この通知を他のゲートウェイ装置から受信したときには自己が保持している前記認証通信路設定中の利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子が前記通知に含まれる前記ネットワークアドレスおよびまたは前記利用者識別子と同一であるか否かを検索する機能と、
この検索する機能の検索結果が同一でないときにはその旨を前記通知の送信元の前記ゲートウェイ装置に応答する機能と、
前記検索する機能の検索結果が同一であるときにはその旨を前記通知の送信元の前記ゲートウェイ装置に応答する機能と、
自己が前記通知の送信元でありこの応答を受信したときにはこの応答の送信元の前記ゲートウェイ装置に対して当該ゲートウェイ装置が保持する重複する前記認証通信路を削除するとともに当該ゲートウェイ装置が保持している重複する前記認証通信路に関する情報を削除する要求を行う機能と、
自己が前記応答の送信元でありこの要求を受信したときには自己が保持する重複する前記認証通信路を削除するとともに自己が保持している重複する前記認証通信路に関する情報を破棄する機能と、
前記要求の送信元に重複する前記認証通信路の該当利用者有りおよび削除完了の旨を応答する機能と、
自己が前記要求の送信元であり前記応答を受信したときには新規の前記認証通信路を設定する機能とを実現させる請求項２３記載のプログラム。

【請求項２６】　認証完了後に前記認証通信路を確立した利用者のネットワークアドレスおよびこのネットワークアドレスに対応する利用者識別子を保持する機能と、
この保持する機能に保持した前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子の情報を他の前記ゲートウェイ装置に通知する機能と、
この通知を他の前記ゲートウェイ装置から受けたときに

は当該認証通信路を設定している前記ゲートウェイ装置の情報および前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子の情報を保持する機能と、

前記認証通信路の設定要求を受信したときには現在自己が保持している全ての前記ゲートウェイ装置で設定されている前記認証通信路を利用している利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子を検索しいずれかが同一のときにはその認証通信路を設定している前記ゲートウェイ装置を確認する機能と、

当該認証通信路を設定している前記ゲートウェイ装置が自己であるときには該当する前記認証通信路を削除するとともに新規に要求された前記認証通信路を設定する機能と、

当該認証通信路を設定している前記ゲートウェイ装置が他の前記ゲートウェイ装置であるときには該当する前記ゲートウェイ装置に対して前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子を設定して前記認証通信路の削除要求を送信する機能と、

自己がこの削除要求を受信したときには、要求中の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子と一致する前記認証通信路を検索してこれを削除し削除完了の旨を前記削除要求元の前記ゲートウェイ装置に応答する機能と、

自己が前記削除要求元でありこの削除完了応答を受信したときには、新規に要求のあった前記認証通信路を設定する機能とを実現させる請求項２３記載のプログラム。

【請求項２７】　情報処理装置にインストールすることにより、その情報処理装置に、請求項１ないし１１のいずれかに記載の中継接続方式に適用される前記情報サーバに相応する機能として、

前記利用者からアクセスがあるときには前記利用者のプライベートネットワークアドレスを用いて前記ゲートウェイ装置に当該利用者の個人認証状態を問い合わせることにより前記利用者識別子を取得する機能を実現させることを特徴とするプログラム。

【請求項２８】　情報処理装置にインストールすることにより、その情報処理装置に、請求項１ないし１１のいずれかに記載の中継接続方式に適用される前記アクセス制御サーバに相応する機能として、

利用者のプライベートアドレスを用いて前記ゲートウェイ装置にこの利用者の個人認証状態を問い合わせることによりこの利用者の利用者識別子を取得する機能と、

前記情報サーバに前記アプリケーションレベルでの個人認証情報としての利用者識別子を送信する機能とを実現させることを特徴とするプログラム。

【請求項２９】　前記個人認証情報を元に前記利用者に対応するアプリケーションを認識する機能と、

この認識する機能により認識したアプリケーションにしたがって前記情報サーバに対してこのアプリケーションレベルでのアクセス制御を行う機能とを実現させる請求項２８記載のプログラム。

【請求項３０】　請求項２１ないし２９のいずれかに記載のプログラムが記録された前記情報処理装置読取可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はネットワークのセキュリティ管理に利用する。特に、プライベートネットワークに利用するに適する。

【０００２】

【従来の技術】プライベートなネットワークアドレスにより制御される私設通信網であり、ネットワークレベル認証および個人認証の双方を行った利用者のみが利用可能な認証通信網では、従来、利用者のネットワークレベルの認証を行い、ネットワークレベルでの認証通信路を設定し、個人認証の完了していない利用者からのアクセス要求があった場合には、この認証通信路を用いて、利用者の個人認証を行い、その上で、利用者による認証通信網の利用を許可する。この従来例を図１４を参照して説明する。図１４は従来の中継接続方式を説明するための図である。以下、図中では、ネットワークをNW、ゲートウェイをGWとして図示する。

【０００３】図１４に示す例では、ゲートウェイ装置（GW装置と図示）３は、利用者端末１からの通信開始要求を受け付けると、ネットワークレベル認証サーバ（NWレベル認証サーバと図示）６に対してその旨をネットワークレベル認証要求として伝達し、ネットワークレベル認証を行う。

【０００４】具体的には、ネットワークレベル認証サーバ６には、あらかじめ正当な利用者のネットワークレベルの認証情報が登録されており、ゲートウェイ装置３から伝達されたネットワークレベル認証要求から正当な利用者であるか否かを判定する。この判定の結果、正当な利用者であることが判定されると、ネットワークレベル認証サーバ６は、ゲートウェイ装置３に対してその旨を通知する。

【０００５】ネットワークレベル認証が完了すると、ゲートウェイ装置３と利用者端末１との間の公衆通信網２に、認証通信路５が形成される。

【０００６】ゲートウェイ装置３にて、利用者端末１より、認証通信路５を介して認証通信網内部の利用を検出した際に、その利用者の個人レベル認証状態が、未認証の場合には、ゲートウェイ装置３は利用者端末１に対し、個人レベル認証を行うように促す。

【０００７】そこで、個人レベル認証を行うために、利用者端末１は認証通信路５を介してゲートウェイ装置３に、個人認証情報を送信する。これを受信したゲートウ

ェイ装置３では、個人認証情報を含む個人レベル認証要求を個人レベル認証サーバ７に転送する。個人レベル認証サーバ７は、個人レベル認証要求を受け取ると個人レベル認証を行う。

【０００８】具体的には、個人レベル認証サーバ７には、あらかじめ利用者の利用者識別子情報を含む個人レベル認証情報が登録されており、ゲートウェイ装置３から転送された個人レベル認証要求に含まれる利用者識別子を含む個人レベル認証情報から正当な利用者からの正当なアクセス要求であるか否かを判定する。この判定の結果、正当な利用者が正当なアクセス要求を行っていることが判定されると、個人レベル認証サーバ７は、ゲートウェイ装置３に対してその旨を通知する。これにより、ネットワークレベル認証および個人レベル認証が完了する。

【０００９】このような認証通信網４と、公衆通信網２との間のゲートウェイ装置３では、ネットワークレベル認証および個人レベル認証が完了すると、ネットワークレベルの識別情報(公衆通信網におけるアドレスであるネットワークアドレス)と個人レベルの識別情報(利用者識別子)をそれぞれ保持し、認証通信網４内部で使用するプライベートネットワークアドレスを割当て、公衆通信網２と認証通信網４との間でのネットワークアドレス変換を行う。

【００１０】情報サーバＡ、Ｂ、Ｃでは、アクセスしてきた利用者のプライベートネットワークアドレスを元にゲートウェイ装置３に対して、利用者の個人認証の状態を問い合わせる。ゲートウェイ装置３は、プライベートネットワークアドレスに基づき利用者識別子を検索して個人認証の状態として、利用者識別子を返送する。情報サーバＡ、Ｂ、Ｃでは、正当に個人認証された利用者からのアクセスを受け入れる。

【００１１】

【発明が解決しようとする課題】このような従来の中継接続方式では、以下のような問題が発生する。利用者端末１より、利用者ａが、認証通信網４内部の情報サーバＡを利用した後に、同一の利用者端末１から、利用者ｂが認証通信網４内部の情報サーバＡを利用するときには、情報サーバＡは、既に利用者ａにより、利用者ａに割当てられたプライベートネットワークアドレスにより認証を済ませており、同一のプライベートネットワークアドレスを利用している利用者ｂが情報サーバＡを利用するときには、改めて認証を行うことはない。したがって、情報サーバ側から利用者の個人認証の状態の特定を正常に行うことは困難である。

【００１２】また、認証通信網内部へアクセスする認証通信路設定後に、個人レベル認証を実行するため、ゲートウェイ装置は、認証通信路上での情報サーバへのアクセスを監視し、アクセスを検出した際に、認証通信路上で実行される様々なアプリケーションから個人レベル認証サーバへ接続するよう誘導する必要があり、そのために、アプリケーション毎の対応が必要となる。したがって、ゲートウェイ装置の処理負荷が大きくなってしまう。

【００１３】さらに、個人レベル認証に誘導し、個人認証を行っている間に受信するパケットをゲートウェイ装置内部に保持し、個人レベル認証完了時に保持しているパケットを認証通信網内部に転送する必要がある。したがって、これもゲートウェイ装置の処理負荷を増大させる要因になる。

【００１４】本発明は、このような背景に行われたものであって、情報サーバ側から利用者を特定することができる中継接続方式を提供することを目的とする。本発明は、認証通信網内における認証状態の不一致または重複を回避することができる中継接続方式を提供することを目的とする。本発明は、ネットワークレベル認証および個人レベル認証の手順を簡単化することができる中継接続方式を提供することを目的とする。本発明は、ゲートウェイ装置の処理負荷を軽減させることができる中継接続方式を提供することを目的とする。

【００１５】

【課題を解決するための手段】本発明は、ネットワークレベルおよび個人レベルでの認証の双方を行った利用者が利用可能でありプライベートネットワークアドレスにより制御され利用者に情報を提供する情報サーバを含む私設通信網としての認証通信網と、この認証通信網にアクセスする利用者端末に接続された公衆通信網と前記認証通信網とを接続するゲートウェイ装置とを備えた中継接続方式である。

【００１６】ここで、本発明の特徴とするところは、ネットワークレベルの認証情報に個人レベルの認証情報を付加した認証情報を保持するネットワークレベル認証サーバが設けられ、前記ネットワークレベル認証サーバは、前記認証情報と併せて個人レベルのアクセス制御情報も付加して保持する手段と、前記ゲートウェイ装置から認証要求として受信した被認証情報を検証しその認証結果に前記アクセス制御情報を付加して前記ゲートウェイ装置に返送する手段とを備え、前記ゲートウェイ装置は、ネットワークレベルの被認証情報に個人レベルの被認証情報を付加した被認証情報および利用者識別子と、この被認証情報の有効期限情報とを前記利用者端末から受信し、前記有効期限情報を検証して前記被認証情報の有効性を確認する手段と、前記利用者識別子および前記被認証情報を用いて前記ネットワークレベル認証サーバに対して前記認証要求を送信する手段と、認証の完了時に認証通信網内部で使用するプライベートネットワークアドレスを前記利用者端末の利用者に割当て、このプライベートネットワークアドレスと、前記ネットワークレベル認証サーバから前記認証結果として返送されたネットワークレベルの認証情報および個人レベルの認証情報

としてのネットワークアドレスおよび利用者識別子をそれぞれ保持するとともにこれらに対応して前記ネットワークレベル認証サーバから前記認証情報とともに返送された前記個人レベルのアクセス制御情報を保持する手段と、認証の完了時に、前記利用者との間に相互に秘密情報を共有し、この秘密情報を利用した暗号通信路である認証通信路を前記利用者端末との間に生成する手段と、前記利用者からの認証通信網内へのアクセスについては前記認証通信路に限定して許容するとともに前記公衆通信網におけるネットワークアドレスと前記認証通信網内部で利用するプライベートアドレスとの間でアドレス変換を行う手段と、前記利用者からの前記認証通信網へのアクセス時に前記利用者のネットワークアドレスから該当する前記アクセス制御情報を検索しこのアクセス制御情報にしたがって前記利用者の前記情報サーバに対するアクセスを制御する手段とを備えたところにある。

【００１７】これにより、ネットワークレベル認証と個人レベル認証とを一つの対にして同時に行うため、情報サーバ側から利用者の特定を行うことができる。また、認証状態の不一致または重複を回避することができる。また、これにより、ネットワークレベル認証および個人レベル認証の手順を簡単化することができる。また、ゲートウェイ装置の処理負荷を軽減させることができる。

【００１８】前記情報サーバは、前記利用者からアクセスがあるときには前記利用者のプライベートネットワークアドレスを用いて前記ゲートウェイ装置に当該利用者の個人認証状態を問い合わせることにより前記利用者識別子を取得する手段を備えることが望ましい。

【００１９】これにより、認証状態の情報がネットワークレベル認証サーバにより一元的に管理されているため、情報サーバ側から利用者を特定できるとともに、認証通信網内における認証状態の不一致または重複を回避することができる。

【００２０】また、前記ゲートウェイ装置は、前記情報サーバが個人レベルの認証状態を解放するまで当該利用者に割当てた認証通信網内のプライベートネットワークアドレスの再割当てを行わない手段を備えることが望ましい。

【００２１】これにより、一人の利用者に対する一つの認証状態に対して複数のプライベートネットワークアドレスが重複することを回避することができるので、認証通信網内における認証状態の不一致を回避することができる。

【００２２】また、前記ゲートウェイ装置は、利用者からの要求に応じて、もしくは、利用者から前記認証通信路を利用した前記認証通信網内部への一定時間以上の無通信を検出した時点で、前記認証通信路を削除する手段を備えることもできる。

【００２３】これにより、利用者の都合によりこれまでの認証通信路を削除し、新たな認証手順の実行に備えることができる。

【００２４】また、前記ゲートウェイ装置は、前記認証通信路の削除を行う際に、当該認証通信路の利用者の利用していた前記情報サーバに対して、当該認証通信路の削除と個人レベルの認証状態の解放とを通知する手段を備え、前記情報サーバは、前記ゲートウェイ装置からの前記通知により、該当する利用者の個人レベルの認証状態を解放する手段を備えることもできる。

【００２５】これにより、ゲートウェイ装置で個人レベルの認証状態を解放した場合の認証通信網内における認証状態の不一致または重複を回避することができる。

【００２６】このようにして、本発明によれば、情報サーバ側から利用者を特定することができる。認証通信網内における認証状態の不一致を回避することができる。ネットワークレベル認証および個人レベル認証の手順を簡単化することができる。ゲートウェイ装置の処理負荷を軽減させることができる。

【００２７】また、前記ゲートウェイ装置は、前記利用者からの前記認証通信路の設定要求を受信した際に、前記ネットワークレベル認証サーバに対してこの設定要求に含まれる利用者識別子および被認証情報および前記利用者のネットワークアドレスを前記認証要求に設定して前記ネットワークレベル認証サーバに送信する手段を備え、前記ネットワークレベル認証サーバは、前記認証要求を受信して前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子を保持する手段と、前記認証要求を受信して当該ネットワークレベル認証サーバにより保持されている通信中の前記認証通信路の情報を検索して前記認証要求中に設定されている前記利用者識別子およびまたは前記ネットワークアドレスにしたがって既に前記認証通信路が設定されているか否かを検出する手段と、同一の前記利用者識別子もしくは前記ネットワークアドレスにより既に前記認証通信路が設定されているときには当該認証通信路を設定している前記ゲートウェイ装置に対して重複する前記認証通信路の削除要求を送信する手段とを備え、前記ゲートウェイ装置は、前記認証通信路の削除要求を受信して該当する認証通信路を検索する手段と、この検索する手段の検索結果により前記該当する認証通信路が検索されたときにはその認証通信路を削除して当該削除完了の応答を前記ネットワークレベル認証サーバに通知する手段とを備え、前記ネットワークレベル認証サーバは、同一の前記利用者識別子もしくは前記ネットワークアドレスにより既に前記認証通信路が設定されていないとき、もしくは、前記削除完了の応答を受信したときには前記認証要求に設定されている前記利用者識別子および前記被認証情報を検証してこの認証の結果に該当利用者のアドレス制御情報を付加して応答する手段を備え、前記ゲートウェイ装置は、このアドレス制御情報が付加された応答を受信して前記認証通信路を設定する手段と、当該認証通

信路設定の通知を前記ネットワークレベル認証サーバに送信する手段とを備え、前記ネットワークレベル認証サーバは、前記認証通信路設定の通知を受信して設定済みの認証通信路情報として前記認証通信路を設定した前記ゲートウェイ装置の識別情報および前記利用者識別子および前記ネットワークアドレスをそれぞれ自己内部に保持する手段を備え、前記ゲートウェイ装置は、前記利用者からの要求に応じて、もしくは、前記利用者から前記認証通信路を利用した前記認証通信網内部への一定時間以上の無通信を検出したときに前記認証通信路を削除する手段と、自己内部に保持している該当認証通信路に関する情報を破棄する手段と、該当認証通信路の削除を前記ネットワークレベル認証サーバに通知する手段とを備え、前記ネットワークレベル認証サーバは、この削除の通知を受信して該当する認証通信路に関する情報を破棄する手段を備えることもできる。

【００２８】このようにして、前記ネットワークレベル認証サーバにて、全ての前記ゲートウェイ装置で設定している前記認証通信路のネットワークアドレスおよびこのネットワークアドレスに対応する利用者識別子を保持することにより、ネットワークアドレスおよび利用者識別子の重複をチェックすることができる。

【００２９】また、前記ゲートウェイ装置は、認証完了後に前記認証通信路を確立した利用者の前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子を保持する手段と、前記認証通信路の設定要求を受信したときに現在自己が設定している前記認証通信路を利用している利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子を検索する手段と、この検索する手段の検索結果により前記設定要求に含まれる利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子と現在自己が設定している前記認証通信路を利用している利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子とが同一であるときには前記自己が設定している既存の前記認証通信路を削除して前記設定要求に基づく前記認証通信路を設定する手段と、前記検索する手段の検索結果により前記設定要求に含まれる利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子と現在自己が設定している前記認証通信路を利用している利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子とが一致しないときには他の前記ゲートウェイ装置に前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子を通知する手段と、この通知を他のゲートウェイ装置から受信したときには自己が保持している前記認証通信路設定中の利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子が前記通知に含まれる前記ネットワークアドレスおよびまたは前記利用者識別子と同一であるか否かを検索する手段と、この検索する手段の検索結果が同一でないときにはその旨を前記通知の送信元の前記ゲートウェイ装置に応答する手段と、前記検索する手段の検索結果が同一であるときには自己が保持する重複する前記認証通信路を削除するとともに自己が保持している重複する前記認証通信路に関する情報を破棄する手段と、前記通知の送信元に重複する前記認証通信路の該当利用者有りおよび削除完了の旨を応答する手段と、自己が前記通知の送信元であり前記応答を受信したときには新規の前記認証通信路を設定する手段とを備えることもできる。

【００３０】このようにして、前記ゲートウェイ装置が自己が設定した前記認証通信路に関する前記利用者のネットワークアドレスおよびこのネットワークアドレスに対応する利用者識別子を保持することにより、ネットワークアドレスおよびまたは利用者識別子の重複をチェックすることができる。

【００３１】あるいは、前記ゲートウェイ装置は、認証完了後に前記認証通信路を確立した利用者の前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子を保持する手段と、前記認証通信路の設定要求を受信したときに現在自己が設定している前記認証通信路を利用している利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子を検索する手段と、この検索する手段の検索結果により前記設定要求に含まれる利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子と現在自己が設定している前記認証通信路を利用している利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子とが同一であるときには前記自己が設定している既存の前記認証通信路を削除して前記設定要求に基づく前記認証通信路を設定する手段と、前記検索する手段の検索結果により前記設定要求に含まれる利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子と現在自己が設定している前記認証通信路を利用している利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子とが一致しないときには他の前記ゲートウェイ装置に前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子を通知する手段と、この通知を他のゲートウェイ装置から受信したときには自己が保持している前記認証通信路設定中の利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子が前記通知に含まれる前記ネットワークアドレスおよびまたは前記利用者識別子と同一であるか否かを検索する手段と、この検索

する手段の検索結果が同一でないときにはその旨を前記通知の送信元の前記ゲートウェイ装置に応答する手段と、前記検索する手段の検索結果が同一であるときにはその旨を前記通知の送信元の前記ゲートウェイ装置に応答する手段と、自己が前記通知の送信元でありこの応答を受信したときにはこの応答の送信元の前記ゲートウェイ装置に対して当該ゲートウェイ装置が保持する重複する前記認証通信路を削除するとともに当該ゲートウェイ装置が保持している重複する前記認証通信路に関する情報を削除する要求を行う手段と、自己が前記応答の送信元でありこの要求を受信したときには自己が保持する重複する前記認証通信路を削除するとともに自己が保持している重複する前記認証通信路に関する情報を破棄する手段と、前記要求の送信元に重複する前記認証通信路の該当利用者有りおよび削除完了の旨を応答する手段と、自己が前記要求の送信元であり前記応答を受信したときには新規の前記認証通信路を設定する手段とを備えてもよい。

【００３２】また、前記ゲートウェイ装置は、認証完了後に前記認証通信路を確立した利用者の前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子を保持する手段と、この保持する手段に保持した前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子の情報を他の前記ゲートウェイ装置に通知する手段と、この通知を他の前記ゲートウェイ装置から受けたときには当該認証通信路を設定している前記ゲートウェイ装置の情報および前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子の情報を保持する手段と、前記認証通信路の設定要求を受信したときには現在自己が保持している全ての前記ゲートウェイ装置で設定されている前記認証通信路を利用している利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子を検索しいずれかが同一のときにはその認証通信路を設定している前記ゲートウェイ装置を確認する手段と、当該認証通信路を設定している前記ゲートウェイ装置が自己であるときには該当する前記認証通信路を削除するとともに新規に要求された前記認証通信路を設定する手段と、当該認証通信路を設定している前記ゲートウェイ装置が他の前記ゲートウェイ装置であるときには該当する前記ゲートウェイ装置に対して前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子を設定して前記認証通信路の削除要求を送信する手段と、自己がこの削除要求を受信したときには、要求中の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子と一致する前記認証通信路を検索してこれを削除し削除完了の旨を前記削除要求元の前記ゲートウェイ装置に応答する手段と、自己が前記削除要求元でありこの削除完了応答を受信したときには、新規に要求のあった前記認証通信路を設定する手段とを備えることもできる。

【００３３】このようにして、全ての前記ゲートウェイ装置が全てのゲートウェイ装置によって設定されている前記認証通信路の前記利用者のネットワークアドレスおよびこのネットワークアドレスに対応する利用者識別子をそれぞれ保持することによりネットワークアドレスおよびまたは利用者識別子の重複をチェックすることができる。

【００３４】また、個人認証の実施がアプリケーションレベルに限定された情報サーバが設けられている場合には、前記ゲートウェイ装置と当該情報サーバとの間にアクセス制御サーバを設けておき、このアクセス制御サーバは、利用者のプライベートアドレスを用いて前記ゲートウェイ装置にこの利用者の個人認証状態を問い合わせることによりこの利用者の利用者識別子を取得する手段と、前記情報サーバに前記アプリケーションレベルでの個人認証情報としての利用者識別子を送信する手段とを備えることが望ましい。

【００３５】この際に、前記アクセス制御サーバは、前記個人認証情報を元に前記利用者に対応するアプリケーションを認識する手段と、この認識する手段により認識したアプリケーションにしたがって前記情報サーバに対してこのアプリケーションレベルでのアクセス制御を行う手段とを備えることが望ましい。

【００３６】これにより、アプリケーションレベルでのみ、個人認証を実施可能な情報サーバに対しても本発明の中継接続方式によるシングルサインオンサービスを提供することができる。

【００３７】本発明の第二の観点は、本発明の中継接続方式に適用され、ネットワークレベルの認証情報に個人レベルの認証情報を付加した認証情報を保持する手段と、前記認証情報と併せて個人レベルのアクセス制御情報も付加して保持する手段と、前記ゲートウェイ装置から認証要求として受信した被認証情報を検証しその認証結果に前記アクセス制御情報を付加して前記ゲートウェイ装置に返送する手段とを備えたことを特徴とするネットワークレベル認証サーバである。

【００３８】前記ゲートウェイ装置が利用者からの前記認証通信路の設定要求を受信した際にこの設定要求に含まれる利用者識別子および被認証情報および前記利用者のネットワークアドレスを設定した前記認証要求を受信して前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子を保持する手段と、前記認証要求を受信して保持されている通信中の前記認証通信路の情報を検索して前記認証要求中に設定されている前記利用者識別子およびまたは前記ネットワークアドレスにしたがって既に前記認証通信路が設定されているか否かを検出する手段と、同一の前記利用者識別子もしくは前記ネットワークアドレスにより既に前記認

証通信路が設定されているときには当該認証通信路を設定している前記ゲートウェイ装置に対して重複する前記認証通信路の削除要求を送信する手段と、同一の前記利用者識別子もしくは前記ネットワークアドレスにより既に前記認証通信路が設定されていないとき、もしくは、前記削除完了の応答を受信したときには前記認証要求に設定されている前記利用者識別子および前記被認証情報を検証してこの認証の結果に該当利用者のアドレス制御情報を付加して前記認証要求または前記削除完了の応答を送信したゲートウェイ装置に応答する手段と、前記ゲートウェイ装置からの前記認証通信路設定の通知を受信して設定済みの認証通信路情報として前記認証通信路を設定した前記ゲートウェイ装置の識別情報および前記利用者識別子および前記ネットワークアドレスをそれぞれ自己内部に保持する手段と、前記ゲートウェイ装置からの前記認証通信路の削除の通知を受信して該当する認証通信路に関する情報を破棄する手段とを備えることが望ましい。

【００３９】本発明の第三の観点は、本発明の中継接続方式に適用され、ネットワークレベルの被認証情報に個人レベルの被認証情報を付加した被認証情報および利用者識別子とこの被認証情報の有効期限情報とを前記利用者端末から受信して前記有効期限を検証して前記被認証情報の有効性を確認する手段と、前記利用者識別子および前記被認証情報を用いて前記ネットワークレベル認証サーバに対して前記認証要求を送信する手段と、認証の完了時に認証通信網内部で使用するプライベートネットワークアドレスを前記利用者に割当てこのプライベートネットワークアドレスと前記ネットワークレベル認証サーバから前記認証結果として返送されたネットワークレベルの認証情報および個人レベルの認証情報としての前記利用者の公衆通信網におけるアドレスであるネットワークアドレスおよび利用者識別子をそれぞれ保持するとともにこれらに対応して前記ネットワークレベル認証サーバから前記認証結果とともに返送された前記個人レベルのアクセス制御情報を保持する手段と、認証の完了時に、前記利用者との間に相互に秘密情報を共有してこの秘密情報を利用した暗号通信路である認証通信路を前記利用者端末との間に生成する手段と、前記利用者からの認証通信網内へのアクセスについては前記認証通信路に限定して許容するとともに前記公衆通信網におけるネットワークアドレスと前記認証通信網内部で利用するプライベートアドレスとの間でアドレス変換を行う手段と、前記利用者からの前記認証通信網へのアクセス時に前記利用者のネットワークアドレスから該当する前記アクセス制御情報を検索しこのアクセス制御情報にしたがって前記利用者の前記情報サーバに対するアクセスを制御する手段とを備えたことを特徴とするゲートウェイ装置である。

【００４０】さらに、認証完了後に前記認証通信路を確立した利用者のネットワークアドレスおよびこのネットワークアドレスに対応する利用者識別子を保持する手段と、前記認証通信路の設定要求を受信したときに現在自己が設定している前記認証通信路を利用している利用者のネットワークアドレスおよびまたはこのネットワークアドレスに対応する利用者識別子を検索する手段と、この検索する手段の検索結果により前記設定要求に含まれる利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子と現在自己が設定している前記認証通信路を利用している利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子とが同一であるときには前記自己が設定している既存の前記認証通信路を削除して前記設定要求に基づく前記認証通信路を設定する手段と、前記検索する手段の検索結果により前記設定要求に含まれる利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子と現在自己が設定している前記認証通信路を利用している利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子とが一致しないときには他の前記ゲートウェイ装置に前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子を通知する手段と、この通知を他のゲートウェイ装置から受信したときには自己が保持している前記認証通信路設定中の利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子が前記通知に含まれる前記ネットワークアドレスおよびまたは前記利用者識別子と同一であるか否かを検索する手段と、この検索する手段の検索結果が同一でないときにはその旨を前記通知の送信元の前記ゲートウェイ装置に応答する手段と、前記検索する手段の検索結果が同一であるときには自己が保持する重複する前記認証通信路を削除するとともに自己が保持している重複する前記認証通信路に関する情報を破棄する手段と、前記通知の送信元に重複する前記認証通信路の該当利用者有りおよび削除完了の旨を応答する手段と、自己が前記通知の送信元であり前記応答を受信したときには新規の前記認証通信路を設定する手段とを備えることが望ましい。

【００４１】あるいは、認証完了後に前記認証通信路を確立した利用者のネットワークアドレスおよびこのネットワークアドレスに対応する利用者識別子を保持する手段と、前記認証通信路の設定要求を受信したときに現在自己が設定している前記認証通信路を利用している利用者のネットワークアドレスおよびまたはこのネットワークアドレスに対応する利用者識別子を検索する手段と、この検索する手段の検索結果により前記設定要求に含まれる利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子と現在自己が設定している前記認証通信路を利用している

利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子とが同一であるときには前記自己が設定している既存の前記認証通信路を削除して前記設定要求に基づく前記認証通信路を設定する手段と、前記検索する手段の検索結果により前記設定要求に含まれる利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子と現在自己が設定している前記認証通信路を利用している利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子とが一致しないときには他の前記ゲートウェイ装置に前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子を通知する手段と、この通知を他のゲートウェイ装置から受信したときには自己が保持している前記認証通信路設定中の利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子が前記通知に含まれる前記ネットワークアドレスおよびまたは前記利用者識別子と同一であるか否かを検索する手段と、この検索する手段の検索結果が同一でないときにはその旨を前記通知の送信元の前記ゲートウェイ装置に応答する手段と、前記検索する手段の検索結果が同一であるときにはその旨を前記通知の送信元の前記ゲートウェイ装置に応答する手段と、自己が前記通知の送信元でありこの応答を受信したときにはこの応答の送信元の前記ゲートウェイ装置に対して当該ゲートウェイ装置が保持する重複する前記認証通信路を削除するとともに当該ゲートウェイ装置が保持している重複する前記認証通信路に関する情報を削除する要求を行う手段と、自己が前記応答の送信元でありこの要求を受信したときには自己が保持する重複する前記認証通信路を削除するとともに自己が保持している重複する前記認証通信路に関する情報を破棄する手段と、前記要求の送信元に重複する前記認証通信路の該当利用者有りおよび削除完了の旨を応答する手段と、自己が前記要求の送信元であり前記応答を受信したときには新規の前記認証通信路を設定する手段とを備えることもできる。

【００４２】あるいは、認証完了後に前記認証通信路を確立した利用者のネットワークアドレスおよびこのネットワークアドレスに対応する利用者識別子を保持する手段と、この保持する手段に保持した前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子の情報を他の前記ゲートウェイ装置に通知する手段と、この通知を他の前記ゲートウェイ装置から受けたときには当該認証通信路を設定している前記ゲートウェイ装置の情報および前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子の情報を保持する手段と、前記認証通信路の設定要求を受信したときには現在自己が保持している全ての前記ゲートウェイ装置で設定されている前記認証通信路を利用している利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子を検索しいずれかが同一のときにはその認証通信路を設定している前記ゲートウェイ装置を確認する手段と、当該認証通信路を設定している前記ゲートウェイ装置が自己であるときには該当する前記認証通信路を削除するとともに新規に要求された前記認証通信路を設定する手段と、当該認証通信路を設定している前記ゲートウェイ装置が他の前記ゲートウェイ装置であるときには該当する前記ゲートウェイ装置に対して前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子を設定して前記認証通信路の削除要求を送信する手段と、自己がこの削除要求を受信したときには、要求中の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子と一致する前記認証通信路を検索してこれを削除し削除完了の旨を前記削除要求元の前記ゲートウェイ装置に応答する手段と、自己が前記削除要求元でありこの削除完了応答を受信したときには、新規に要求のあった前記認証通信路を設定する手段とを備えることもできる。

【００４３】本発明の第四の観点は、本発明の中継接続方式に適用され、前記利用者からアクセスがあるときには前記利用者のプライベートネットワークアドレスを用いて前記ゲートウェイ装置に当該利用者の個人認証状態を問い合わせることにより前記利用者識別子を取得する手段を備えたことを特徴とする情報サーバである。

【００４４】本発明の第五の観点は、本発明の中継接続方式に適用され、前記ゲートウェイ装置と個人認証の実施がアプリケーションレベルに限定された情報サーバとの間に設けられ、利用者のプライベートアドレスを用いて前記ゲートウェイ装置にこの利用者の個人認証状態を問い合わせることによりこの利用者の利用者識別子を取得する手段と、前記情報サーバに前記アプリケーションレベルでの個人認証情報としての利用者識別子を送信する手段とを備えたことを特徴とするアクセス制御サーバである。

【００４５】前記個人認証情報を元に前記利用者に対応するアプリケーションを認識する手段と、この認識する手段により認識したアプリケーションにしたがって前記情報サーバに対してこのアプリケーションレベルでのアクセス制御を行う手段とを備えることが望ましい。

【００４６】本発明の第六の観点は、情報処理装置にインストールすることにより、その情報処理装置に、本発明の中継接続方式に適用される前記ネットワークレベル認証サーバに相応する機能として、ネットワークレベルの認証情報に個人レベルの認証情報を付加した認証情報を保持する機能と、前記認証情報と併せて個人レベルのアクセス制御情報も付加して保持する機能と、前記ゲートウェイ装置から認証要求として受信した被認証情報を検証しその認証結果に前記アクセス制御情報を付加して

前記ゲートウェイ装置に返送する機能とを実現させることを特徴とするプログラムである。

【００４７】さらに、このプログラムは、前記ゲートウェイ装置が利用者からの前記認証通信路の設定要求を受信した際にこの設定要求に含まれる利用者識別子および被認証情報および前記利用者のネットワークアドレスを設定した前記認証要求を受信して前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子を保持する機能と、前記認証要求を受信して保持されている通信中の前記認証通信路の情報を検索して前記認証要求中に設定されている前記利用者識別子およびまたは前記ネットワークアドレスにしたがって既に前記認証通信路が設定されているか否かを検出する機能と、同一の前記利用者識別子もしくは前記ネットワークアドレスにより既に前記認証通信路が設定されているときには当該認証通信路を設定している前記ゲートウェイ装置に対して重複する前記認証通信路の削除要求を送信する機能と、同一の前記利用者識別子もしくは前記ネットワークアドレスにより既に前記認証通信路が設定されていないとき、もしくは、前記削除完了の応答を受信したときには前記認証要求に設定されている前記利用者識別子および前記被認証情報を検証してこの認証の結果に該当利用者のアドレス制御情報を付加して前記認証要求または前記削除完了の応答を送信したゲートウェイ装置に応答する機能と、前記ゲートウェイ装置からの前記認証通信路設定の通知を受信して設定済みの認証通信路情報として前記認証通信路を設定した前記ゲートウェイ装置の識別情報および前記利用者識別子および前記ネットワークアドレスをそれぞれ自己内部に保持する機能と、前記ゲートウェイ装置からの前記認証通信路の削除の通知を受信して該当する認証通信路に関する情報を破棄する機能とを実現させることが望ましい。

【００４８】あるいは、情報処理装置にインストールすることにより、その情報処理装置に、本発明の中継接続方式に適用される前記ゲートウェイ装置に相応する機能として、ネットワークレベルの被認証情報に個人レベルの被認証情報を付加した被認証情報および利用者識別子とこの被認証情報の有効期限情報とを前記利用者端末から受信して前記有効期限を検証して前記被認証情報の有効性を確認する機能と、前記利用者識別子および前記被認証情報を用いて前記ネットワークレベル認証サーバに対して前記認証要求を送信する機能と、認証の完了時に認証通信網内部で使用するプライベートネットワークアドレスを前記利用者に割当てこのプライベートネットワークアドレスと前記ネットワークレベル認証サーバから前記認証結果として返送されたネットワークレベルの認証情報および個人レベルの認証情報としての前記利用者の公衆通信網におけるアドレスであるネットワークアドレスおよび利用者識別子をそれぞれ保持するとともにこれらに対応して前記ネットワークレベル認証サーバから前記認証結果とともに返送された前記個人レベルのアクセス制御情報を保持する機能と、認証の完了時に、前記利用者との間に相互に秘密情報を共有し、この秘密情報を利用した暗号通信路である認証通信路を前記利用者端末との間に生成する機能と、前記利用者からの認証通信網内へのアクセスについては前記認証通信路に限定して許容するとともに前記公衆通信網におけるネットワークアドレスと前記認証通信網内部で利用するプライベートアドレスとの間でアドレス変換を行う機能と、前記利用者からの前記認証通信網へのアクセス時に前記利用者のネットワークアドレスから該当する前記アクセス制御情報を検索しこのアクセス制御情報にしたがって前記利用者の前記情報サーバに対するアクセスを制御する機能とを実現させることを特徴とするプログラムである。

【００４９】さらに、このプログラムは、認証完了後に前記認証通信路を確立した利用者のネットワークアドレスおよびこのネットワークアドレスに対応する利用者識別子を保持する機能と、前記認証通信路の設定要求を受信したときに現在自己が設定している前記認証通信路を利用している利用者のネットワークアドレスおよびまたはこのネットワークアドレスに対応する利用者識別子を検索する機能と、この検索する機能の検索結果により前記設定要求に含まれる利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子と現在自己が設定している前記認証通信路を利用している利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子とが同一であるときには前記自己が設定している既存の前記認証通信路を削除して前記設定要求に基づく前記認証通信路を設定する機能と、前記検索する機能の検索結果により前記設定要求に含まれる利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子と現在自己が設定している前記認証通信路を利用している利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子とが一致しないときには他の前記ゲートウェイ装置に前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子を通知する機能と、この通知を他のゲートウェイ装置から受信したときには自己が保持している前記認証通信路設定中の利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子が前記通知に含まれる前記ネットワークアドレスおよびまたは前記利用者識別子と同一であるか否かを検索する機能と、この検索する機能の検索結果が同一でないときにはその旨を前記通知の送信元の前記ゲートウェイ装置に応答する機能と、前記検索する機能の検索結果が同一であるときには自己が保持する重複する前記認証通信路を削除するとともに自己が保持している重複する前記認証通信路に関する情報を破棄する機能と、前

記通知の送信元に重複する前記認証通信路の該当利用者有りおよび削除完了の旨を応答する機能と、自己が前記通知の送信元であり前記応答を受信したときには新規の前記認証通信路を設定する機能とを実現させることが望ましい。

【００５０】あるいは、認証完了後に前記認証通信路を確立した利用者のネットワークアドレスおよびこのネットワークアドレスに対応する利用者識別子を保持する機能と、前記認証通信路の設定要求を受信したときに現在自己が設定している前記認証通信路を利用している利用者のネットワークアドレスおよびまたはこのネットワークアドレスに対応する利用者識別子を検索する機能と、この検索する機能の検索結果により前記設定要求に含まれる利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子と現在自己が設定している前記認証通信路を利用している利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子とが同一であるときには前記自己が設定している既存の前記認証通信路を削除して前記設定要求に基づく前記認証通信路を設定する機能と、前記検索する機能の検索結果により前記設定要求に含まれる利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子と現在自己が設定している前記認証通信路を利用している利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子とが一致しないときには他の前記ゲートウェイ装置に前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子を通知する機能と、この通知を他のゲートウェイ装置から受信したときには自己が保持している前記認証通信路設定中の利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子が前記通知に含まれる前記ネットワークアドレスおよびまたは前記利用者識別子と同一であるか否かを検索する機能と、この検索する機能の検索結果が同一でないときにはその旨を前記通知の送信元の前記ゲートウェイ装置に応答する機能と、前記検索する機能の検索結果が同一であるときにはその旨を前記通知の送信元の前記ゲートウェイ装置に応答する機能と、自己が前記通知の送信元でありこの応答を受信したときにはこの応答の送信元の前記ゲートウェイ装置に対して当該ゲートウェイ装置が保持する重複する前記認証通信路を削除するとともに当該ゲートウェイ装置が保持している重複する前記認証通信路に関する情報を削除する要求を行う機能と、自己が前記応答の送信元でありこの要求を受信したときには自己が保持する重複する前記認証通信路を削除するとともに自己が保持している重複する前記認証通信路に関する情報を破棄する機能と、前記要求の送信元に重複する前記認証通信路の該当利用者有りおよび削除完了の旨を応答する機能と、自己が前記要求の送信元であり前記応答を受信したときには新規の前記認証通信路を設定する機能とを実現させることもできる。

【００５１】あるいは、認証完了後に前記認証通信路を確立した利用者のネットワークアドレスおよびこのネットワークアドレスに対応する利用者識別子を保持する機能と、この保持する機能に保持した前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子の情報を他の前記ゲートウェイ装置に通知する機能と、この通知を他の前記ゲートウェイ装置から受けたときには当該認証通信路を設定している前記ゲートウェイ装置の情報および前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子の情報を保持する機能と、前記認証通信路の設定要求を受信したときには現在自己が保持している全ての前記ゲートウェイ装置で設定されている前記認証通信路を利用している利用者の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子を検索しいずれかが同一のときにはその認証通信路を設定している前記ゲートウェイ装置を確認する機能と、当該認証通信路を設定している前記ゲートウェイ装置が自己であるときには該当する前記認証通信路を削除するとともに新規に要求された前記認証通信路を設定する機能と、当該認証通信路を設定している前記ゲートウェイ装置が他の前記ゲートウェイ装置であるときには該当する前記ゲートウェイ装置に対して前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子を設定して前記認証通信路の削除要求を送信する機能と、自己がこの削除要求を受信したときには、要求中の前記ネットワークアドレスおよびまたはこのネットワークアドレスに対応する前記利用者識別子と一致する前記認証通信路を検索してこれを削除し削除完了の旨を前記削除要求元の前記ゲートウェイ装置に応答する機能と、自己が前記削除要求元でありこの削除完了応答を受信したときには、新規に要求のあった前記認証通信路を設定する機能とを実現させることもできる。

【００５２】あるいは、情報処理装置にインストールすることにより、その情報処理装置に、本発明の中継接続方式に適用される前記情報サーバに相応する機能として、前記利用者からアクセスがあるときには前記利用者のプライベートネットワークアドレスを用いて前記ゲートウェイ装置に当該利用者の個人認証状態を問い合わせることにより前記利用者識別子を取得する機能を実現させることを特徴とするプログラムである。

【００５３】あるいは、情報処理装置にインストールすることにより、その情報処理装置に、本発明の中継接続方式に適用される前記アクセス制御サーバに相応する機能として、利用者のプライベートアドレスを用いて前記ゲートウェイ装置にこの利用者の個人認証状態を問い合わせることによりこの利用者の利用者識別子を取得する

機能と、前記情報サーバに前記アプリケーションレベルでの個人認証情報としての利用者識別子を送信する機能とを実現させることを特徴とするプログラムである。

【００５４】さらに、このプログラムは、前記個人認証情報を元に前記利用者に対応するアプリケーションを認識する機能と、この認識する機能により認識したアプリケーションにしたがって前記情報サーバに対してこのアプリケーションレベルでのアクセス制御を行う機能とを実現させることが望ましい。

【００５５】本発明の第七の観点は、本発明のプログラムが記録された前記情報処理装置読取可能な記録媒体である。本発明のプログラムを記録した本発明の記録媒体を用いて本発明のプログラムを前記情報処理装置にインストールすることができる。また、本発明のプログラムを保持するサーバからネットワークを介して前記情報処理装置が本発明のプログラムをダウンロードすることによっても前記情報処理装置は本発明のプログラムをインストールすることができる。

【００５６】

【発明の実施の形態】本発明実施例の中継接続方式を図１および図１２を参照して説明する。図１は本発明実施例の中継接続方式の全体構成図である。図１２は本発明第六実施例の中継接続方式の全体構成図である。

【００５７】本発明は、ネットワークレベルおよび個人レベルでの認証の双方を行った利用者が利用可能でありプライベートネットワークアドレスにより制御され利用者に情報を提供する情報サーバA、B、Cを含む私設通信網としての認証通信網４と、この認証通信網４にアクセスする利用者端末１に接続された公衆通信網２と認証通信網４とを接続するゲートウェイ装置３とを備えた中継接続方式である。

【００５８】ここで、本発明の特徴とするところは、ネットワークレベルの認証情報に個人レベルの認証情報を付加した認証情報を保持するネットワークレベル認証サーバ６が設けられ、ネットワークレベル認証サーバ６は、前記認証情報と併せて個人レベルのアクセス制御情報も付加して保持し、ゲートウェイ装置３から認証要求として受信した被認証情報を検証しその認証結果に前記アクセス制御情報を付加してゲートウェイ装置３に返送し、ゲートウェイ装置３は、ネットワークレベルの被認証情報に個人レベルの被認証情報を付加した被認証情報および利用者識別子と、この被認証情報の有効期限情報とを利用者端末１から受信し、この被認証情報の有効期限情報により、この被認証情報の有効性を検証後、この利用者識別子および被認証情報を用いてネットワークレベル認証サーバ６に対して前記認証要求を送信し、認証の完了時に認証通信網４内部で使用するプライベートネットワークアドレスを利用者端末１の利用者に割当て、このプライベートネットワークアドレスと、ネットワークレベル認証サーバ６から前記認証結果として返送されたネットワークレベルの認証情報および個人レベルの認証情報としての前記利用者のネットワークアドレスおよび利用者識別子をそれぞれ保持するとともにこれらに対応してネットワークレベル認証サーバ６から前記認証結果とともに返送された前記個人レベルのアクセス制御情報を保持し、認証の完了時に、前記利用者との間に相互に秘密情報を共有し、この秘密情報を利用した暗号通信路である認証通信路５を利用者端末１との間に生成し、前記利用者からの認証通信網４内へのアクセスについては認証通信路５に限定して許容するとともに公衆通信網２におけるネットワークアドレスと認証通信網４内部で利用するプライベートアドレスとの間でアドレス変換を行い、前記利用者からの認証通信網４へのアクセス時に前記利用者のネットワークアドレスから前記アクセス制御情報を取得しこのアクセス制御情報にしたがって前記利用者の情報サーバA、B、Cに対するアクセスを制御するところにある。

【００５９】本発明実施例の中継接続方式を実現するためには、情報処理装置であるコンピュータ装置にインストールすることにより、そのコンピュータ装置に、本発明の中継接続方式に適用されるネットワークレベル認証サーバ６、ゲートウェイ装置３、情報サーバA、B、C、D、E、アクセス制御サーバ８に相応する機能を実現させるプログラムを用いて、前記コンピュータ装置を本発明のネットワークレベル認証サーバ６、ゲートウェイ装置３、情報サーバA、B、C、D、E、アクセス制御サーバ８に相応する装置として本発明の中継接続方式を実現することができる。なお、前記プログラムを前記コンピュータ装置が読み取り可能な記録媒体に記録しておき、この記録媒体によって前記コンピュータ装置に前記プログラムをインストールしたり、あるいは、前記プログラムを保持するサーバからネットワークを介して前記コンピュータ装置が前記プログラムをダウンロードしてインストールすることができる。

【００６０】以下では、本発明実施例をさらに詳細に説明する。

【００６１】（第一実施例）本発明第一実施例の中継接続方式の構成を図１を参照して説明する。利用者端末１は、公衆通信網２に接続する。認証通信網４は、プライベートネットワークアドレスにより制御される私設通信網で、ゲートウェイ装置３、ネットワークレベル認証サーバ６を含む。また、認証通信網４は、内部に情報サーバA、B、Cを含む情報サーバ通信網＃１、＃２を含む。ネットワークレベルおよび個人レベルでの認証の双方を行った利用者に対しては、ゲートウェイ装置３と利用者端末１との間に認証通信路５が設定される。ゲートウェイ装置３では、認証通信路５を利用しての通信に対し、公衆通信網２から、認証通信網４内部のプライベートネットワークアドレスへのアドレス変換、各情報サーバ通信網＃１、＃２に対してのアクセス制御を行う。

【００６２】次に、本発明第一実施例の中継接続方式の動作を図２～図６を参照して説明する。図２は利用者端末１が利用者の認証通信網４内へのアクセスを検出してから認証通信路５が形成されるまでの動作を示すシーケンス図である。図３は利用者端末１の利用者がアプリケーションの利用を開始し通信を継続している過程の動作を示すシーケンス図である。図４は利用者端末１からの通信が一定時間途絶えた場合の動作を示すシーケンス図である。図５および図６は利用者ａの情報サーバＡの利用後に利用者ｂが情報サーバＡを利用する場合の動作を示すシーケンス図である。

【００６３】図１および図２～図６のシーケンス図を参照して本発明第一実施例の中継接続方式の全体動作について詳細に説明する。まず、認証通信網４を利用する利用者について、ネットワークレベルの認証情報に、個人レベルの認証情報を付加した認証情報、また、その利用者の個人レベルのアクセス制御情報を、認証通信網４内のネットワークレベル認証サーバ６にあらかじめ登録する。ゲートウェイ装置３には、個人レベルのアクセス制御情報に応じたアクセス可能な情報サーバ通信網＃１、＃２のリストをあらかじめ設定する。

【００６４】図２に示すように、前記利用者が認証通信網４内部の情報サーバＡにアクセスを要求すると利用者端末１は、ゲートウェイ装置３に対して通信開始要求を行う。次に、通信開始要求を受けたゲートウェイ装置３は、内部で認証用の情報を生成してその応答に設定する。

【００６５】利用者端末１では、その間に、前記利用者からの個人レベルの認証情報の入力を受け付ける。その後、入力された個人レベルの認証情報とネットワークレベルの認証情報およびゲートウェイ装置３から受信した認証用の情報を合わせて一つの被認証情報を生成し、当該利用者の利用者識別子と当該利用者の被認証情報の有効期限情報とを合わせて認証要求信号を作成し、ゲートウェイ装置３に対して認証要求を送信する。

【００６６】ゲートウェイ装置３は、受信した前記利用者の被認証情報の有効期限情報により、この被認証情報の有効性を検証した後、利用者識別子および被認証情報を認証要求としてネットワークレベル認証サーバ６に送信する。

【００６７】ネットワークレベル認証サーバ６では認証要求として受信した各情報を元に、ネットワークレベル認証サーバ６内部に保持している認証情報の再計算を行って認証を行う。認証後、認証結果とともに、利用者のアクセス制御種別をゲートウェイ装置３に対して通知する。

【００６８】ゲートウェイ装置３では、認証正常であった前記利用者に対し、認証サーバ通信網４内部で使用するプライベートネットワークアドレスを割当て、利用者識別子および前記利用者の公衆通信網２でのネットワークアドレス情報および認証通信網４を利用する際に認証通信網４内部で使用するプライベートネットワークアドレス情報およびアクセス制御種別を内部で保持する。また、認証正常であった前記利用者と、共有の秘密情報を交換する。これにより、利用者端末１とゲートウェイ装置３との間に共有の秘密情報を用いて暗号化された認証通信路５が設定される。

【００６９】認証通信路５の設定中の動作を図３に示す。前記利用者が、認証サーバ通信網４内の情報サーバＡを使用する際は、ゲートウェイ装置３は、公衆通信網２と認証通信網４との間で、ネットワークアドレスの変換を行うＮＡＴ(network address translate)として動作する。

【００７０】また、通信中の利用者をネットワークレベルで管理し、通信の継続により、前記情報をゲートウェイ装置３内部に通信中保持して認証状態を維持する。

【００７１】また、ゲートウェイ装置３では、前記利用者の行き先のアドレスを見て、保持しているアクセス制御種別にしたがったアクセス制御を行う。ゲートウェイ装置３は、アクセス制御種別ごとに、アクセス可能な情報サーバ通信網＃１、＃２のリストを持つ。前記利用者が、情報サーバ通信網＃１にのみアクセス可能なアクセス制御種別で登録されている場合には、ゲートウェイ装置３にて、ネットワークレベルでアクセス制御を行うため、前記利用者は、登録時の契約にしたがった、情報サーバ通信網＃１に属する情報サーバＡ、もしくは情報サーバＢにのみアクセス可能となる。

【００７２】情報サーバＡでは、前記利用者からのアクセスが発生した際に、その通信の発信者のアドレス情報であるゲートウェイ装置３の割当てたプライベートネットワークアドレスを元に、ゲートウェイ装置３に対し、当該利用者の利用者識別子を問い合わせる。

【００７３】ゲートウェイ装置３では、情報サーバＡからの利用者識別子の問い合わせに対し、プライベートネットワークアドレスから、利用者識別子を検索し、利用者識別子を返送する。

【００７４】情報サーバＡでは、前記利用者からのアクセス中、ゲートウェイ装置３から取得したプライベートネットワークアドレスおよび利用者識別子を保持し、当該利用者のプライベートネットワークアドレスを利用した通信が行われている間、当該利用者の個人レベルの認証状態を認証済みとして保持する。

【００７５】通信切断時の動作を図４に示す。ゲートウェイ装置３では、利用者端末１からの認証通信路５の切断要求を受信すると該当する利用者の認証状態を解放する。

【００７６】情報サーバＡでは、認証通信路の切断を認識できないため、前記利用者からの通信の状況を監視し、一定時間以上の無通信を検出した時点で、前記プライベートネットワークアドレスと利用者識別子との対情

報を削除して個人レベル認証状態を解放する。

【００７７】そのため、ゲートウェイ装置３では、情報サーバＡにて、無通信の監視時間が満了し、個人レベルの認証状態が解放されるまで、前記利用者に割当てた認証通信網４内のプライベートネットワークアドレスの再割当てを行わないよう、認証通信路５の切断後、情報サーバＡで無通信の監視時間が満了するまでプライベートネットワークアドレスの割当てを抑制する。

【００７８】図５に同一の利用者端末１もしくは同一のネットワークアドレスにより複数の利用者ａおよびｂからアクセスがあった場合の動作を示す。利用者端末１では、利用者ａが利用していた同一端末上で、異なる利用者ｂの認証通信網４へのアクセスを検出した場合には元の認証通信路５を削除する。ゲートウェイ装置３では元の利用者ａの認証通信路５に関する情報を解放する。

【００７９】利用者端末１は、解放処理完了後、新規に利用する利用者ｂにより認証通信路５設定のための処理を行い、認証通信路５を改めて設定する。

【００８０】図６に、利用者端末１に対して認証通信路５を設定している状態で、同一の利用者端末１もしくは同一のネットワークアドレスにより認証通信路５の設定要求を受けた場合の処理を示す。

【００８１】ゲートウェイ装置３では、認証通信路５を設定している利用者端末１と同一のネットワークアドレスにより利用者端末１から認証通信網４へのアクセスを検出した場合には元の認証通信路５に関する情報を解放し、新規に利用する利用者ｂにより認証通信路５設定のための認証処理を受け入れて、認証通信路５を改めて設定する。

【００８２】（第二実施例）本発明第二実施例を図７を参照して説明する。図７は利用者端末１からの認証通信路切断要求にしたがって認証通信路５を切断する動作を示すシーケンス図である。

【００８３】前述の第一実施例では、情報サーバＡ、Ｂ、Ｃとゲートウェイ装置３で個人認証状態をあわせるために無通信時間の検出を用いたが、第二実施例では、情報サーバＡにて、アプリケーションレベルでの情報サーバＡの使用状態を監視している場合に、情報サーバＡでは、利用者が、情報サーバＡ上のアプリケーションを使用している間のみ、認証状態を保持し、アプリケーションの使用完了を検出した時点で、個人レベルの認証状態を解放する。

【００８４】図７に示すように、アプリケーションレベルの利用状態が利用中の状態で、前記利用者から、認証通信路５の切断要求を受信した場合には、ゲートウェイ装置３より、当該利用者の利用している情報サーバＡに対し、認証通信路５の切断による解放を通知することで、ゲートウェイ装置３および情報サーバＡともに個人認証状態を解放することができる。

【００８５】ゲートウェイ装置３では、個人認証状態を解放するのに伴って、該当する利用者のネットワークレベル認証状態も解放される。したがって、ゲートウェイ装置３では、認証状態を維持している間は保持されていた該当する利用者のネットワークアドレスおよび利用者識別子が削除される。さらに、該当する利用者のアクセス制御情報も削除される。このようにすることで、ゲートウェイ装置３では、認証通信路５の切断後、即座にプライベートネットワークアドレスの再割当てが可能である。

【００８６】（第三実施例）本発明第三実施例を図８を参照して説明する。図８は本発明第三実施例のネットワークアドレスおよび利用者識別子の重複チェック手順を示すシーケンス図である。本発明第三実施例は、ネットワークレベル認証サーバ６が全てのゲートウェイ装置３により設定されている認証通信路５の利用者のネットワークアドレスおよびこのネットワークアドレスに対応する利用者識別子を保持することにより、ネットワークアドレスおよび利用者識別子の重複をチェックする手順を示す実施例である。

【００８７】図８に示すように、ゲートウェイ装置３は、利用者からの認証通信路５の設定要求を受信した際に、ネットワークレベル認証サーバ６に対してこの設定要求に含まれる利用者識別子および被認証情報および利用者のネットワークアドレスを認証要求に設定してネットワークレベル認証サーバ６に送信する。

【００８８】ネットワークレベル認証サーバ６は、この認証要求を受信して前記利用者のネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子を保持し、当該ネットワークレベル認証サーバ６により保持されている通信中の認証通信路５の情報を検索して前記認証要求中に設定されている前記利用者識別子および前記ネットワークアドレスにしたがって既に認証通信路５が設定されているか否かを検出し、同一の前記利用者識別子もしくは前記ネットワークアドレスにより既に認証通信路５が設定されているときには当該認証通信路５を設定しているゲートウェイ装置３に対して重複する認証通信路５の削除要求を送信する。

【００８９】ゲートウェイ装置３は、認証通信路５の削除要求を受信して該当する認証通信路５を検索し、この検索結果により該当する認証通信路５が検索されたときにはその認証通信路５を削除して当該削除完了の応答をネットワークレベル認証サーバ６に通知する。

【００９０】この通知を受け取ったネットワークレベル認証サーバ６は、同一の前記利用者識別子もしくは前記ネットワークアドレスにより既に認証通信路５が設定されていないとき、もしくは、前記削除完了の応答を受信したときには前記認証要求に設定されている前記利用者識別子および前記被認証情報を検証してこの認証の結果に該当利用者のアドレス制御情報を付加して応答する。

【００９１】ゲートウェイ装置３は、このアドレス制御

情報が付加された応答を受信して認証通信路５を設定し、当該認証通信路設定の通知をネットワークレベル認証サーバ６に送信する。

【００９２】ネットワークレベル認証サーバ６は、前記認証通信路設定の通知を受信して設定済みの認証通信路情報として認証通信路５を設定したゲートウェイ装置３の識別情報および前記利用者識別子および前記ネットワークアドレスをそれぞれ自己内部に保持する。

【００９３】ゲートウェイ装置３は、前記利用者からの要求に応じて、もしくは、前記利用者から認証通信路５を利用した認証通信網４内部への一定時間以上の無通信を検出したときに認証通信路５を削除し、自己内部に保持している該当認証通信路５に関する情報を破棄し、該当認証通信路５の削除をネットワークレベル認証サーバ６に通知する。

【００９４】ネットワークレベル認証サーバ６は、この削除の通知を受信して該当する認証通信路５に関する情報を破棄する。

【００９５】（第四実施例）本発明第四実施例を図９および図１０を参照して説明する。図９および図１０は本発明第四実施例のネットワークアドレスおよび利用者識別子の重複チェック手順を示すシーケンス図である。本発明第四実施例は、各ゲートウェイ装置３が自己が設定した認証通信路５の利用者のネットワークアドレスおよびこのネットワークアドレスに対応する利用者識別子を保持することにより、ネットワークアドレスおよび利用者識別子の重複をチェックする手順を示す実施例である。

【００９６】図９に示すように、ゲートウェイ装置３は、認証完了後に認証通信路５を確立した利用者のネットワークアドレスおよびこのネットワークアドレスに対応する利用者識別子を保持し、認証通信路５の設定要求を受信したときに現在自己が設定している認証通信路５を利用している利用者のネットワークアドレスおよびこのネットワークアドレスに対応する利用者識別子を検索し、この検索結果により前記設定要求に含まれる利用者の前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子と現在自己が設定している認証通信路５を利用している利用者の前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子とが同一であるときには前記自己が設定している既存の認証通信路５を削除して前記設定要求に基づく認証通信路５を設定する。あるいは、前記検索結果により前記設定要求に含まれる利用者の前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子と現在自己が設定している認証通信路５を利用している利用者の前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子とが一致しないときには他のゲートウェイ装置３に前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子を通知する。

【００９７】ゲートウェイ装置３がこの通知を他のゲートウェイ装置３から受信したときには自己が保持している認証通信路５設定中の利用者のネットワークアドレスおよびこのネットワークアドレスに対応する利用者識別子が前記通知に含まれる前記ネットワークアドレスおよび前記利用者識別子と同一であるか否かを検索し、この検索結果が同一でないときにはその旨を前記通知の送信元のゲートウェイ装置３に応答する。あるいは、前記検索結果が同一であるときには自己が保持する重複する認証通信路５を削除するとともに自己が保持している重複する認証通信路５に関する情報を破棄し、前記通知の送信元に重複する認証通信路５の該当利用者有りおよび削除完了の旨を応答する。

【００９８】自己が前記通知の送信元であり前記応答を受信したゲートウェイ装置３は、新規の認証通信路５を設定する。

【００９９】あるいは、図１０に示すように、ゲートウェイ装置３は、前記検索結果により前記設定要求に含まれる利用者の前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子と現在自己が設定している前記認証通信路を利用している利用者の前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子とが一致しないときには他のゲートウェイ装置３に前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子を通知し、この通知を受け取ったゲートウェイ装置３は、自己が保持している認証通信路５設定中の利用者の前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子が前記通知に含まれる前記ネットワークアドレスおよび前記利用者識別子と同一であるか否かを検索し、この検索結果が同一でないときにはその旨を前記通知の送信元のゲートウェイ装置３に応答し、前記検索結果が同一であるときにはその旨を前記通知の送信元のゲートウェイ装置３に応答する。

【０１００】自己が前記通知の送信元でありこの応答を受信したゲートウェイ装置３は、この応答の送信元のゲートウェイ装置３に対して当該ゲートウェイ装置３が保持する重複する認証通信路５を削除するとともに当該ゲートウェイ装置３が保持している重複する認証通信路５に関する情報を削除する要求を行う。

【０１０１】自己が前記応答の送信元でありこの要求を受信したゲートウェイ装置３は、自己が保持する重複する認証通信路５を削除するとともに自己が保持している重複する認証通信路５に関する情報を破棄し、前記要求の送信元に重複する認証通信路５の該当利用者有りおよび削除完了の旨を応答する。

【０１０２】自己が前記要求の送信元であり前記応答を受信したゲートウェイ装置３は、新規の認証通信路５を

設定する。

【０１０３】（第五実施例）本発明第五実施例を図１１を参照して説明する。図１１は本発明第五実施例のネットワークアドレスおよび利用者識別子の重複チェック手順を示すシーケンス図である。本発明第五実施例は、全てのゲートウェイ装置３が設定した認証通信路５の利用者のネットワークアドレスおよびこのネットワークアドレスに対応する利用者識別子をそれぞれ保持することにより、ネットワークアドレスおよび利用者識別子の重複をチェックする手順を示す実施例である。

【０１０４】図１１に示すように、ゲートウェイ装置３は、認証完了後に認証通信路５を確立した利用者のネットワークアドレスおよびこのネットワークアドレスに対応する利用者識別子を保持し、この保持した前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子の情報を他のゲートウェイ装置３に通知する。

【０１０５】この通知を他のゲートウェイ装置３から受けたときには当該認証通信路５を設定しているゲートウェイ装置３の情報および前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子の情報を保持する。

【０１０６】認証通信路５の設定要求を受信したゲートウェイ装置３は、現在自己が保持している全てのゲートウェイ装置３で設定されている認証通信路５を利用している利用者の前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子を検索しいずれかが同一のときにはその認証通信路５を設定しているゲートウェイ装置３を確認する。

【０１０７】当該認証通信路５を設定しているゲートウェイ装置３が自己であるときには該当する認証通信路５を削除するとともに新規に要求された認証通信路５を設定する。

【０１０８】当該認証通信路５を設定しているゲートウェイ装置３が他のゲートウェイ装置３であるときには該当するゲートウェイ装置３に対して前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子を設定して認証通信路３の削除要求を送信する。

【０１０９】自己がこの削除要求を受信したゲーウェイ装置３は、要求中の前記ネットワークアドレスおよびこのネットワークアドレスに対応する前記利用者識別子と一致する認証通信路５を検索してこれを削除し削除完了の旨を前記削除要求元の前記ゲートウェイ装置３に応答する。

【０１１０】自己が前記削除要求元でありこの削除完了応答を受信したゲートウェイ装置３は、新規に要求のあった認証通信路５を設定する。

【０１１１】（第六実施例）本発明第六実施例を図１２および図１３を参照して説明する。図１２は第六実施例の中継接続方式の全体構成図である。図１３は第六実施例のアクセス制御サーバの動作を説明するためのシーケンス図である。

【０１１２】第六実施例は、個人認証の実施がアプリケーションレベルに限定された情報サーバD、Eが設けられている例である。この場合には、ゲートウェイ装置３と当該情報サーバD、Eとの間にアクセス制御サーバ８を設けておき、このアクセス制御サーバ８は、利用者のプライベートアドレスを用いてゲートウェイ装置３にこの利用者の個人認証状態を問い合わせることによりこの利用者の利用者識別子を取得し、情報サーバD、Eに前記アプリケーションレベルでの個人認証情報としての利用者識別子を送信する。この際に、アクセス制御サーバ８は、前記個人認証情報を元に前記利用者に対応するアプリケーションを認識し、この認識したアプリケーションにしたがって情報サーバD、Eに対してこのアプリケーションレベルでのアクセス制御を行う。

【０１１３】これにより、アプリケーションレベルでのみ、個人認証を実施可能な情報サーバD、Eに対しても本発明の中継接続方式によるシングルサインオンサービスを提供することができる。

【０１１４】（実施例まとめ）本発明実施例の中継接続方式を用いることにより、ネットワークレベル認証と個人レベル認証を同時に実行し、ゲートウェイ装置３で認証状態を一括して管理することにより、ネットワークレベル認証と個人レベル認証の認証状態の不一致または重複を回避することができる。また、これにより、認証手順を簡単化することができる。

【０１１５】また、情報サーバA、B、Cにて、個人レベル認証の状態を保持している間は、ゲートウェイ装置３にて対応する利用者に割り当てたプライベートネットワークアドレスを割当てないことで認証通信網４内部での認証状態の不一致または重複を防ぐことができる。また、情報サーバA、B、C側で利用者ａまたはｂ　を特定することができる。

【０１１６】また、ネットワークレベルで、個人レベルのアクセス制御を実行することができる。

【０１１７】認証通信網４を利用する利用者に対してネットワークレベルの認証通信路５設定時に個人レベル認証を行うため、個人レベル認証の実行を画一化できるため、認証手順を簡単化することができる。

【０１１８】認証通信路５設定時に、個人レベル認証を行うため、ゲートウェイ装置３を介して、認証通信網４内部へアクセスする通信は、個人レベル認証の完了した通信となるため、認証状態の不一致または重複を回避することができる。

【０１１９】情報サーバA、B、Cにて、個人認証を保持している間は、対応するプライベートネットワークアドレスの割当てを行わないため、情報サーバA、B、Cとゲートウェイ装置３との間の認証状態の不一致または

重複を回避することができる。

【０１２０】ゲートウェイ装置３にて、認証通信網４内部にアクセスする通信を監視し、個人レベル認証の完了していない利用者に対し、使用するアプリケーションに応じて個人レベル認証に誘導するなどのアプリケーションに対応した個人レベル認証への誘導処理を行う必要が無くなり、ゲートウェイ装置３の処理負荷を軽減させることができる。

【０１２１】ゲートウェイ装置３にて、個人レベル認証を、認証通信路５設定以前に行うため、個人レベル認証への誘導を検出した際に受信した通信パケットをゲートウェイ装置３内に保留し、個人レベル認証完了後に、認証通信網４内部に転送するという処理を行う必要が無くなり、ゲートウェイ装置３の処理負荷を軽減させることができる。

【０１２２】

【発明の効果】以上説明したように、本発明によれば、情報サーバ側から利用者を特定することができる。認証通信網内における認証状態の不一致を回避することができる。ネットワークレベル認証および個人レベル認証の手順を簡単化することができる。本発明は、ゲートウェイ装置の処理負荷を軽減させることができる。

【図面の簡単な説明】

【図１】本発明実施例の中継接続方式の全体構成図。

【図２】利用者端末が利用者の認証通信網内へのアクセスを検出してから認証通信路が形成されるまでの動作を示すシーケンス図。

【図３】利用者端末の利用者がアプリケーションの利用を開始し通信を継続している過程の動作を示すシーケンス図。

【図４】利用者端末からの認証通信路切断要求にしたがって認証通信路を切断し、情報サーバＡで、利用者の無通信により個人レベルの認証状態を解放する動作を示すシーケンス図。

【図５】利用者ａの情報サーバＡの利用後に利用者ｂが情報サーバＡを利用する場合の動作を示すシーケンス図。

【図６】利用者ａの情報サーバＡの利用後に利用者ｂが情報サーバＡを利用する場合の動作を示すシーケンス図。

【図７】利用者端末からの認証通信路切断要求にしたがって認証通信路を切断し、利用者の利用した情報サーバに対し、個人レベルの認証状態の解放通知により個人認証を解放する動作を示すシーケンス図。

【図８】本発明第三実施例のネットワークアドレスおよび利用者識別子の重複チェック手順を示すシーケンス図。

【図９】本発明第四実施例のネットワークアドレスおよび利用者識別子の重複チェック手順を示すシーケンス図。

【図１０】本発明第四実施例のネットワークアドレスおよび利用者識別子の重複チェック手順を示すシーケンス図。

【図１１】本発明第五実施例のネットワークアドレスおよび利用者識別子の重複チェック手順を示すシーケンス図。

【図１２】本発明第六実施例の中継接続方式の全体構成図。

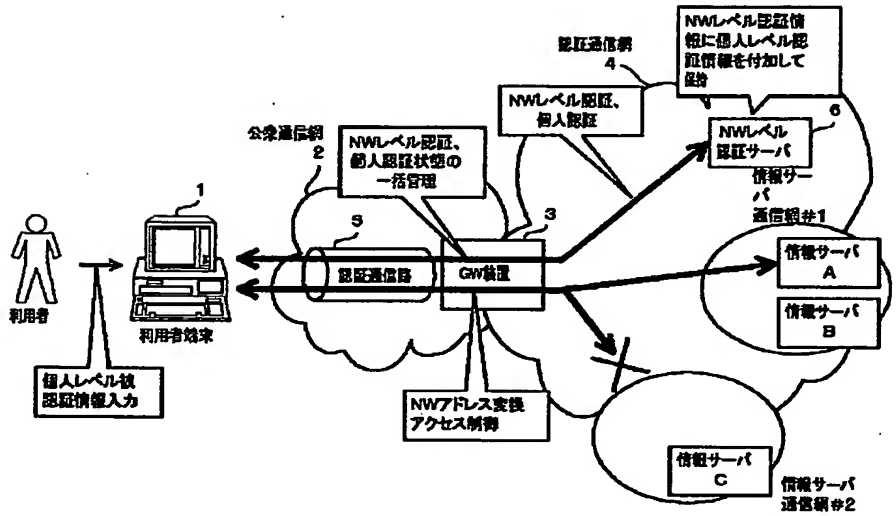
【図１３】本発明第六実施例のアクセス制御サーバの動作を説明するためのシーケンス図。

【図１４】従来の中継接続方式を説明するための図。

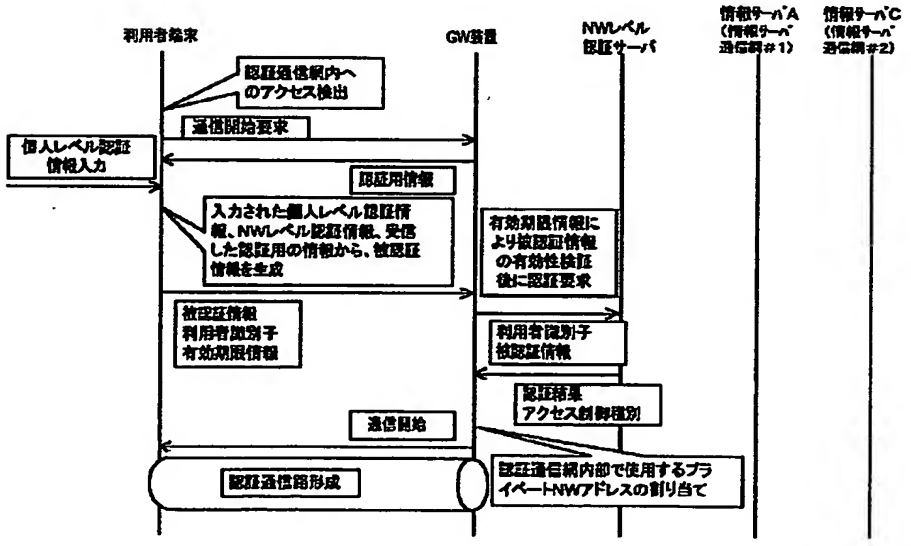
【符号の説明】

１　利用者端末
２　公衆通信網
３　ゲートウェイ装置
４　認証通信網
５　認証通信路
６　ネットワークレベル認証サーバ
７　個人レベル認証サーバ
８　アクセス制御サーバ
Ａ、Ｂ、Ｃ、Ｄ、Ｅ　情報サーバ
ａ、ｂ　利用者
＃１、＃２　情報サーバ通信網

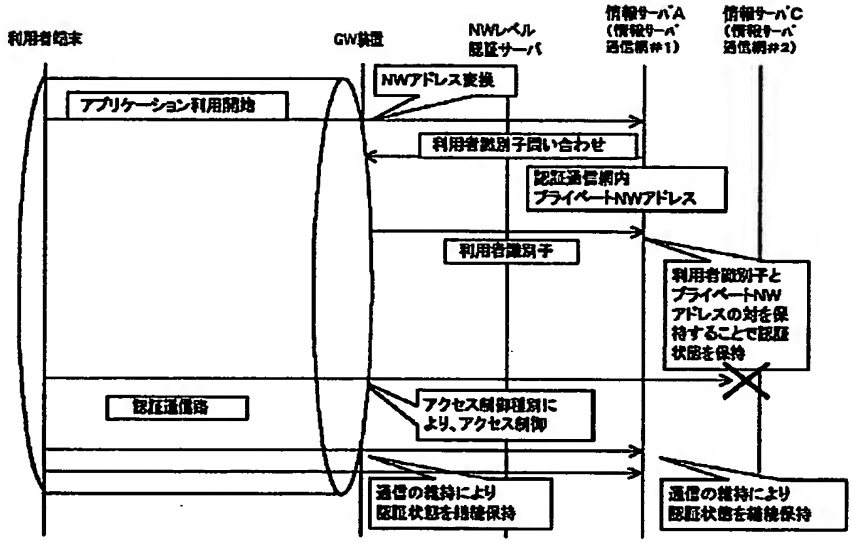
【図１】


NWレベル認証情報に個人レベル認証情報を付加して保持
認証通信網
4
NWレベル認証、個人認証
NWレベル認証サーバ
6
情報サーバ通信網#1
公衆通信網
2
NWレベル認証、個人認証状態の一括管理
1
3
5
利用者
利用者端末
認証通信路
GW装置
情報サーバA
情報サーバB
個人レベル被認証情報入力
NWアドレス変換アクセス制御
情報サーバC
情報サーバ通信網#2

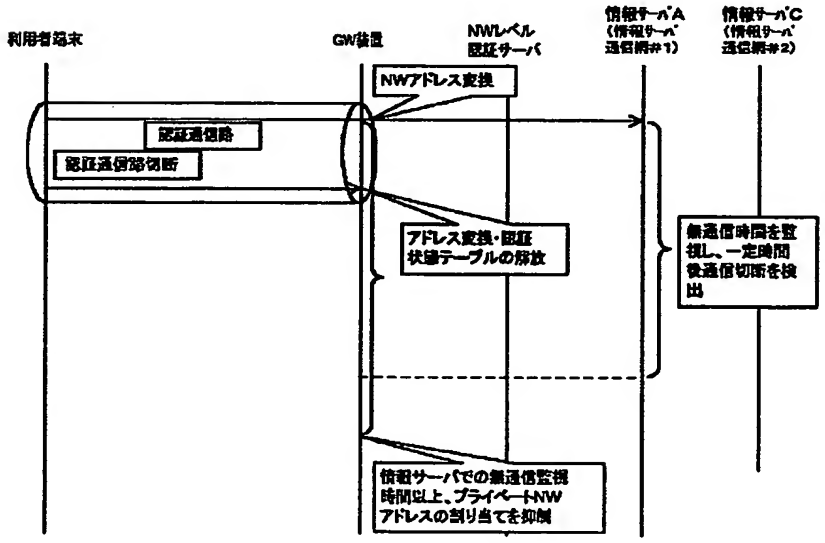
【図２】


利用者端末
GW装置
NWレベル認証サーバ
情報サーバA（情報サーバ通信網#1）
情報サーバC（情報サーバ通信網#2）
認証通信網内へのアクセス検出
通信開始要求
個人レベル認証情報入力
認証用情報
入力された個人レベル認証情報、NWレベル認証情報、受信した認証用の情報から、被認証情報を生成
有効期限情報により被認証情報の有効性検証後に認証要求
被認証情報
利用者識別子
有効期限情報
利用者識別子
被認証情報
認証結果
アクセス制御種別
通信開始
認証通信路形成
認証通信網内部で使用するプライベートNWアドレスの割り当て

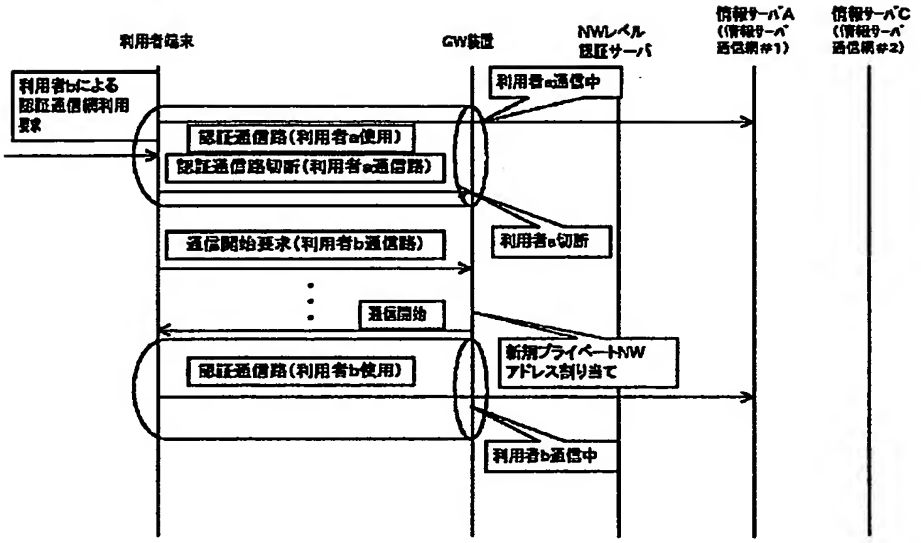
【図３】


利用者端末
GW装置
NWレベル
認証サーバ
情報サーバA
(情報サーバ
通信網#1)
情報サーバC
(情報サーバ
通信網#2)
NWアドレス変換
アプリケーション利用開始
利用者識別子問い合わせ
認証通信網内
プライベートNWアドレス
利用者識別子
利用者識別子と
プライベートNW
アドレスの対を保
持することで認証
状態を保持
認証通信路
アクセス制御理別に
より、アクセス制御
通信の維持により
認証状態を継続保持
通信の維持により
認証状態を継続保持

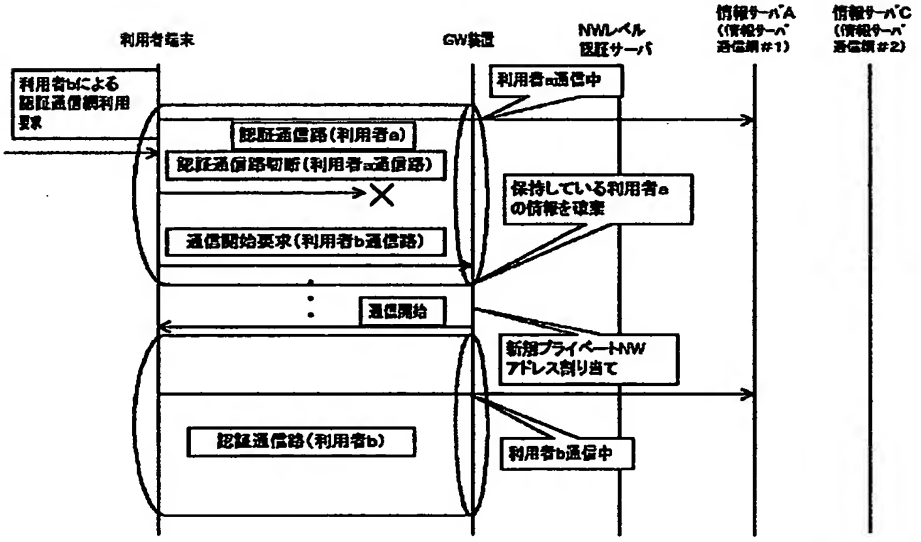
【図４】


利用者端末
GW装置
NWレベル
認証サーバ
情報サーバA
(情報サーバ
通信網#1)
情報サーバC
(情報サーバ
通信網#2)
NWアドレス変換
認証通信路
認証通信路切断
アドレス変換・認証
状態テーブルの解放
無通信時間を監
視し、一定時間
後通信切断を検
出
情報サーバでの無通信監視
時間以上、プライベートNW
アドレスの割り当てを抑制

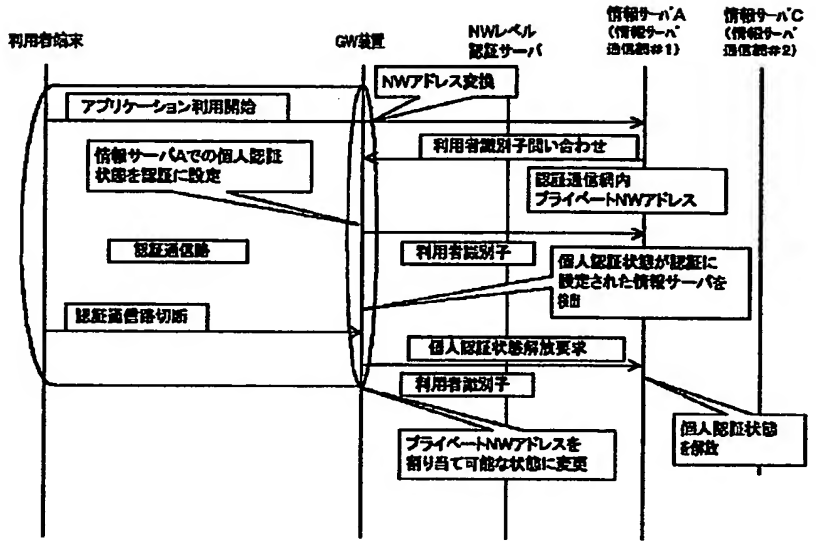
【図５】


利用者端末
GW装置
NWレベル
認証サーバ
情報サーバA
(情報サーバ
通信網#1)
情報サーバC
(情報サーバ
通信網#2)
利用者aによる
認証通信網利用
要求
利用者a通信中
認証通信路(利用者a使用)
認証通信路切断(利用者a通信路)
利用者a切断
通信開始要求(利用者b通信路)
通信開始
新規プライベートNW
アドレス割り当て
認証通信路(利用者b使用)
利用者b通信中

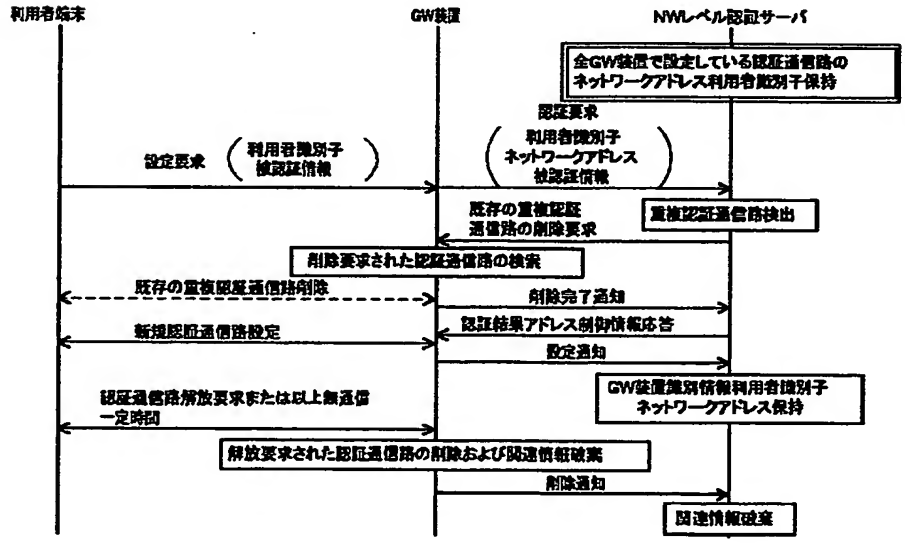
【図６】


利用者端末
GW装置
NWレベル
認証サーバ
情報サーバA
(情報サーバ
通信網#1)
情報サーバC
(情報サーバ
通信網#2)
利用者aによる
認証通信網利用
要求
利用者a通信中
認証通信路(利用者a)
認証通信路切断(利用者a通信路)
保持している利用者a
の情報を破棄
通信開始要求(利用者b通信路)
通信開始
新規プライベートNW
アドレス割り当て
認証通信路(利用者b)
利用者b通信中

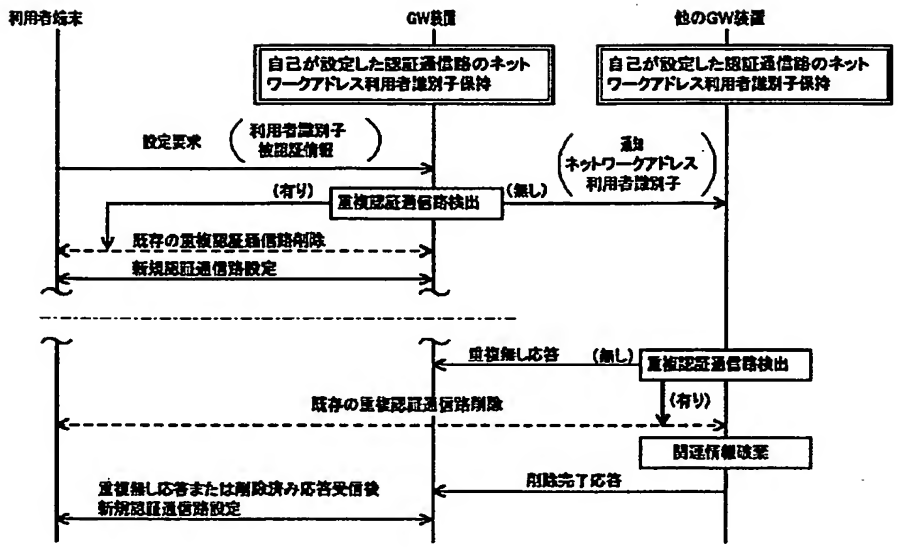
【図７】


利用者端末
GW装置
NWレベル認証サーバ
情報サーバA
情報サーバC
NWアドレス変換
アプリケーション利用開始
利用者識別子問い合わせ
情報サーバAでの個人認証状態を認証に設定
認証通信網内プライベートNWアドレス
認証通信路
利用者識別子
個人認証状態が認証に設定された情報サーバを検出
認証通信路切断
個人認証状態解放要求
利用者識別子
プライベートNWアドレスを割り当て可能な状態に変更
個人認証状態を保持

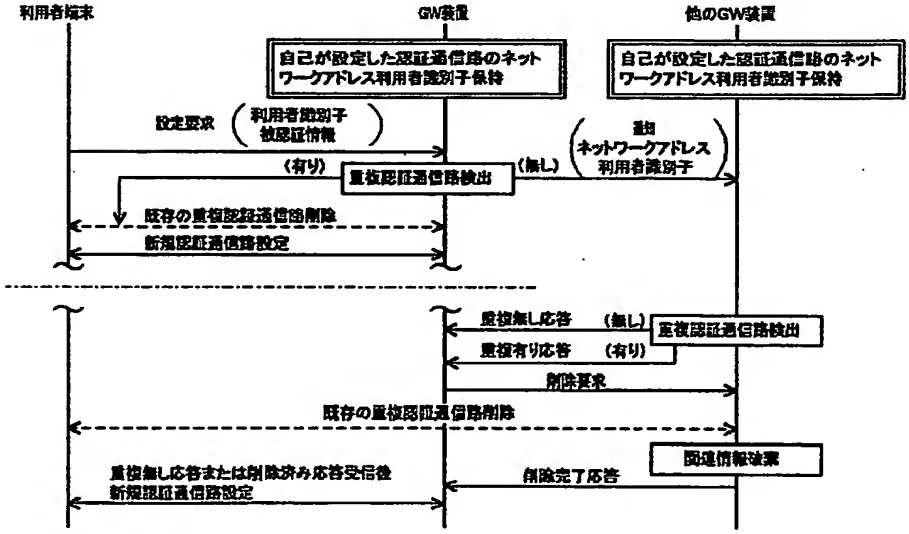
【図８】


利用者端末
GW装置
NWレベル認証サーバ
全GW装置で設定している認証通信路のネットワークアドレス利用者識別子保持
認証要求
設定要求
利用者識別子
被認証情報
利用者識別子
ネットワークアドレス
被認証情報
既存の重複認証通信路の削除要求
重複認証通信路検出
削除要求された認証通信路の検索
既存の重複認証通信路削除
削除完了通知
新規認証通信路設定
認証結果アドレス制御情報応答
設定通知
GW装置識別情報利用者識別子ネットワークアドレス保持
認証通信路解放要求または以上無通信一定時間
解放要求された認証通信路の削除および関連情報破棄
削除通知
関連情報破棄

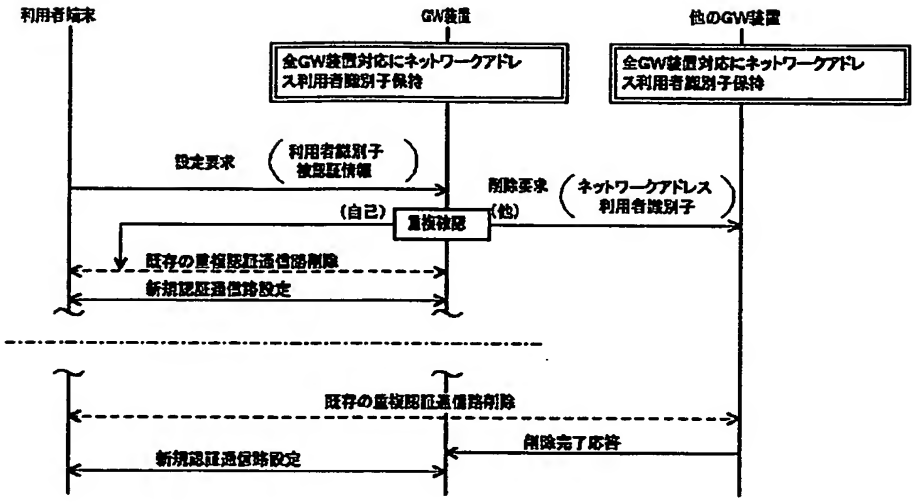
【図９】


利用者端末
GW装置
他のGW装置
自己が設定した認証通信路のネットワークアドレス利用者識別子保持
自己が設定した認証通信路のネットワークアドレス利用者識別子保持
設定要求
利用者識別子
被認証情報
通知
ネットワークアドレス
利用者識別子
(有り)
重複認証通信路検出
(無し)
既存の重複認証通信路削除
新規認証通信路設定
重複無し応答
(無し)
重複認証通信路検出
既存の重複認証通信路削除
(有り)
関連情報破棄
削除完了応答
重複無し応答または削除済み応答受信後
新規認証通信路設定

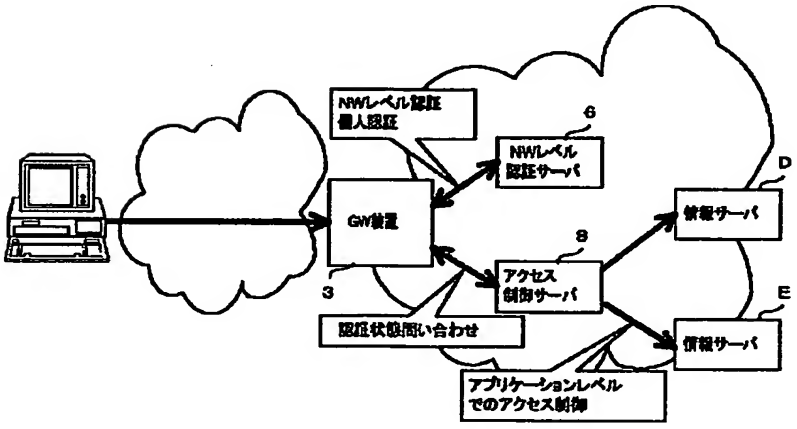
【図１０】


利用者端末
GW装置
他のGW装置
自己が設定した認証通信路のネットワークアドレス利用者識別子保持
自己が設定した認証通信路のネットワークアドレス利用者識別子保持
設定要求
利用者識別子
被認証情報
通知
ネットワークアドレス
利用者識別子
(有り)
重複認証通信路検出
(無し)
既存の重複認証通信路削除
新規認証通信路設定
重複無し応答
(無し)
重複認証通信路検出
重複有り応答
(有り)
削除要求
既存の重複認証通信路削除
関連情報破棄
重複無し応答または削除済み応答受信後
新規認証通信路設定
削除完了応答

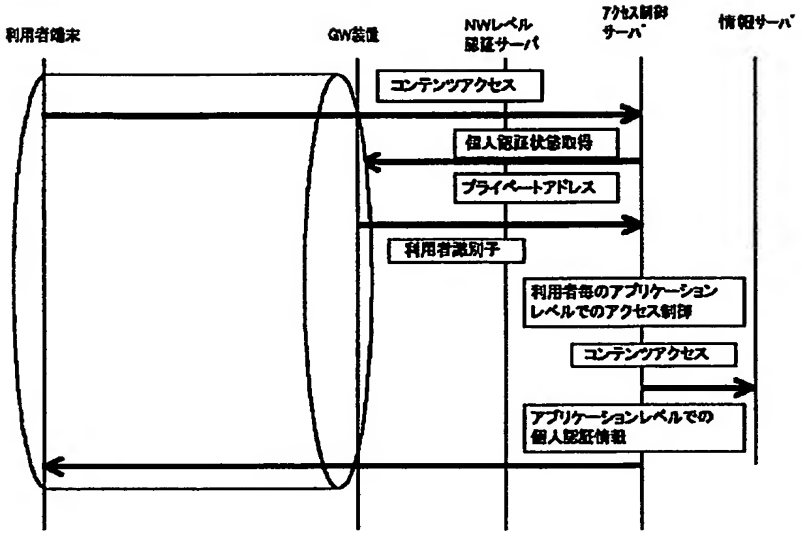
【図１１】


利用者端末
GW装置
他のGW装置
全GW装置対応にネットワークアドレス利用者識別子保持
全GW装置対応にネットワークアドレス利用者識別子保持
設定要求
利用者識別子
被認証情報
削除要求
ネットワークアドレス
利用者識別子
(自己)
(他)
重複確認
既存の重複認証通信路削除
新規認証通信路設定
既存の重複認証通信路削除
削除完了応答
新規認証通信路設定

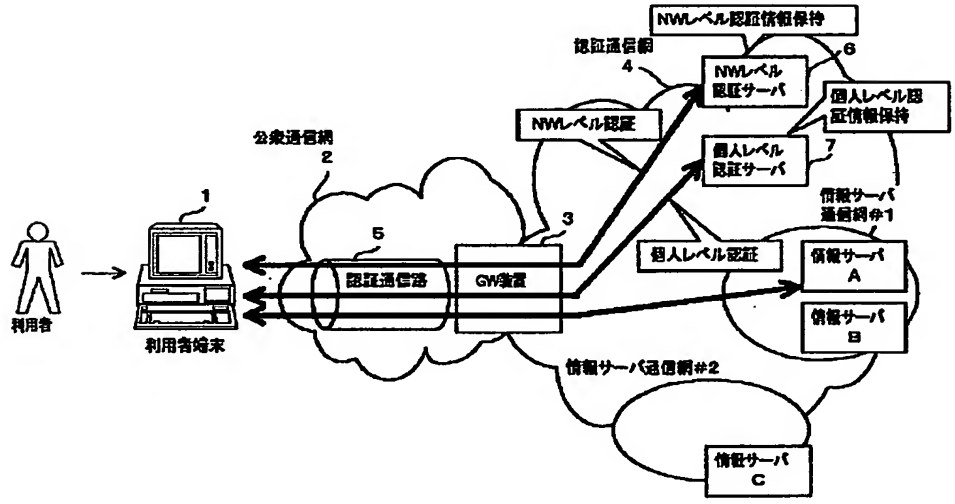
【図１２】


NWレベル認証
個人認証
6
NWレベル
認証サーバ
D
GW装置
情報サーバ
8
アクセス
制御サーバ
3
E
認証状態問い合わせ
情報サーバ
アプリケーションレベル
でのアクセス制御

【図１３】



【図１４】



フロントページの続き

(72)発明者　井上　拓也
東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内

(72)発明者　山田　順之介
東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内

(72)発明者　溝口　陽一
東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内

Ｆターム(参考)　5K030 GA15 HD03 HD06 LD20